Reverse engineering di protocolli radio proprietari: dalle basi al design di un ricetrasmettitore in hardware

Federico Maggi, @phretor
https://maggi.cc - https://ggad.it

TREND MICRO™ | research

HACK IN BO® Winter 2019 Edition
13ª EDIZIONE


GO!

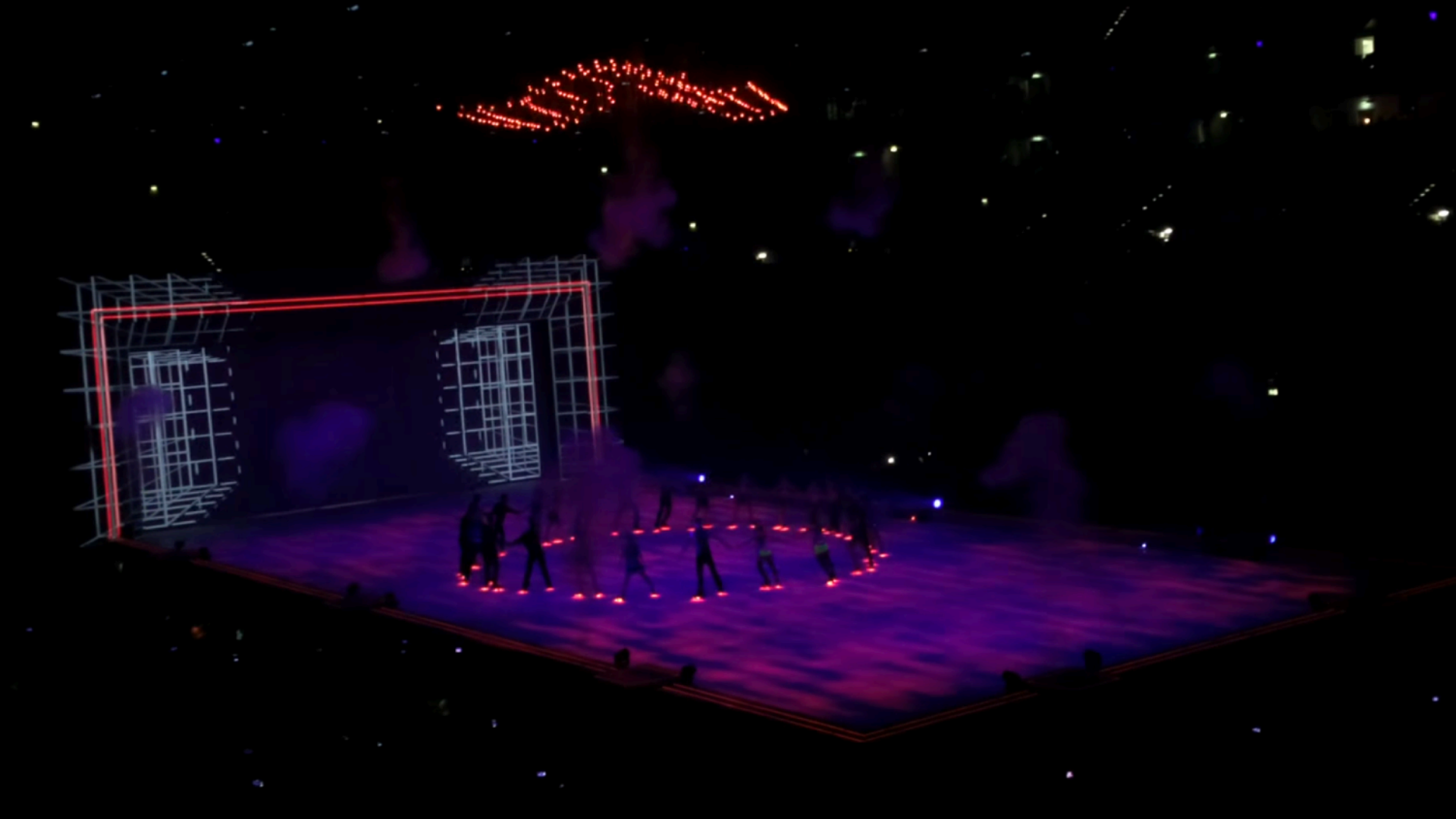

COMPUTER SECURITY CONFERENCE
NO HAT

https://mcts.maggi.cc

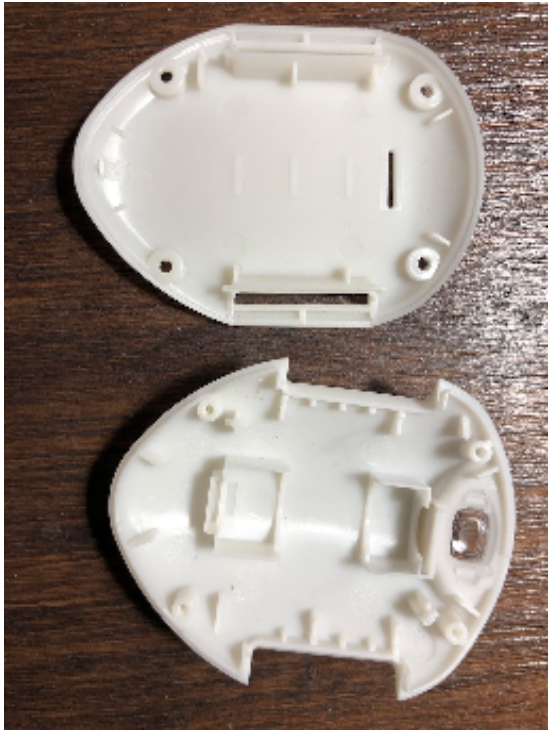
Codice (pubblico a fine gioco):
https://is.gd/mctshib19

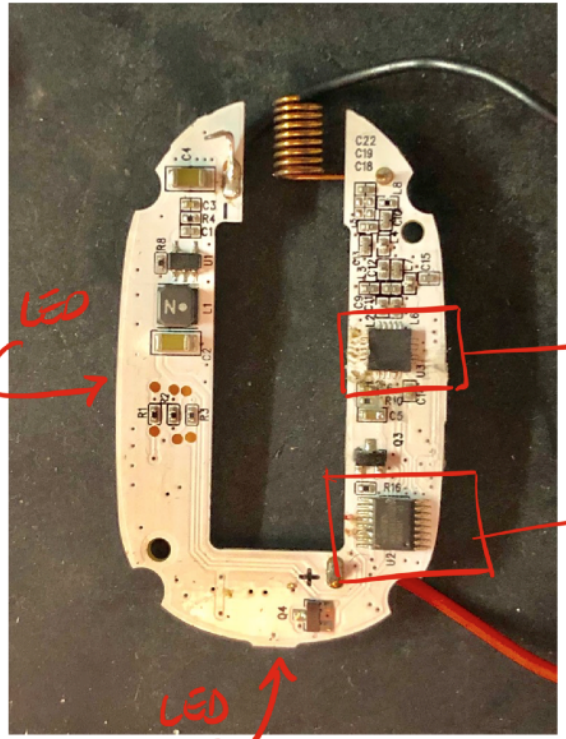

HITB


HITB



Cheap, small, ...but similar to their big brothers!

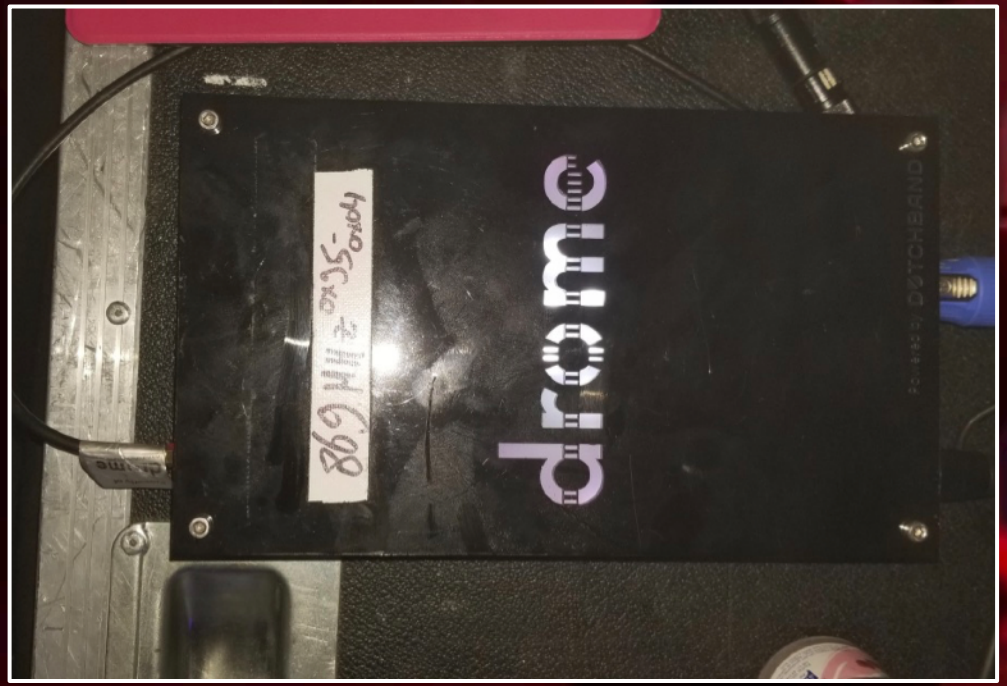


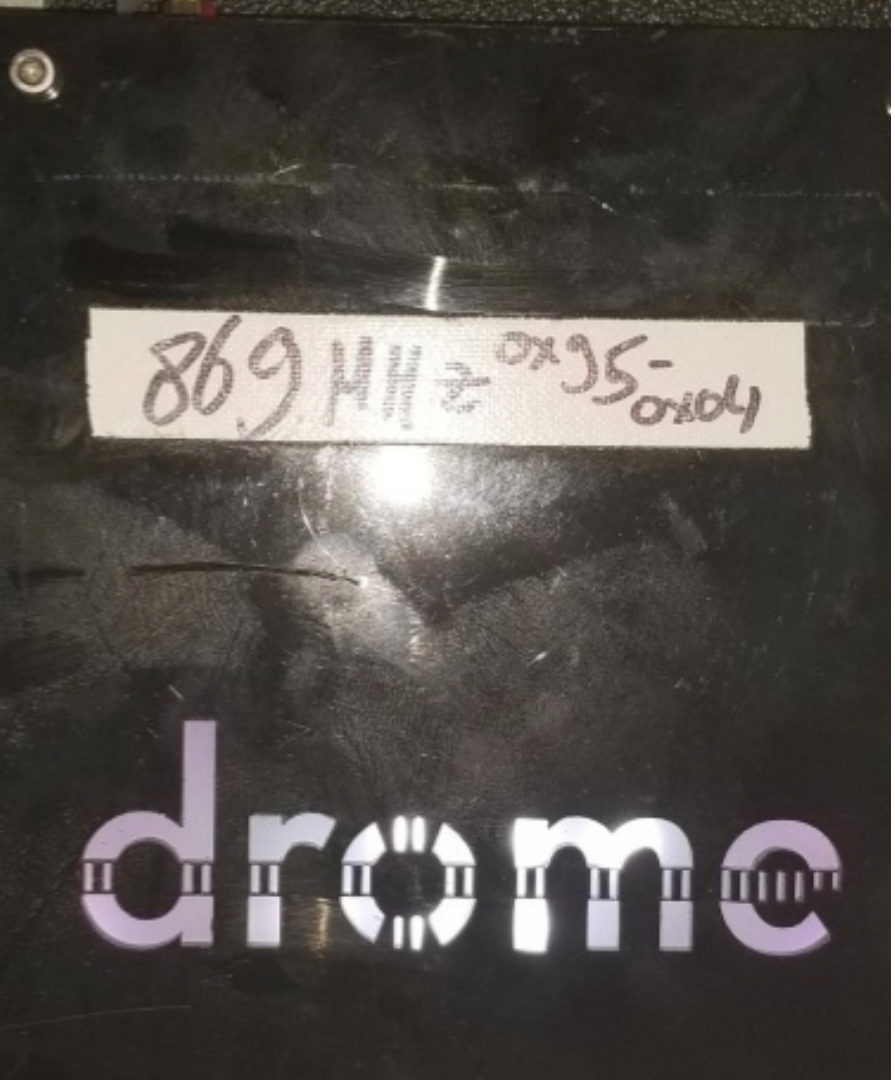

LED
LED
RADIO TRANSCEIVER
MICRO CONTROLLER

Perfect for **learning**!

Perfect for **learning**!

From **zero** to "complete"
reverse engineering!




869 MHz 0x95-0x04
drome

www.dromesurroundlight.com

drome
surround light

home | join the party | technology

Drome up your party

The future is now

The Drome LED wristband is the future of live entertainment.

It creates a richer involvement of the audience to the show by making them part of it. The wristband consists of bright multi-colour LEDs and an ultra high intensity white strobe LED. A high-energy battery system in combination with state-of-the-art LEDs result in effects that will light up the whole venue. Effects like smooth colour changes and rapid ultra bright strobe flashes will make the audience go wild!

www.dromesurroundlight.com

drome
surround light

home | join the party | technology

We helped some greats

Heineken

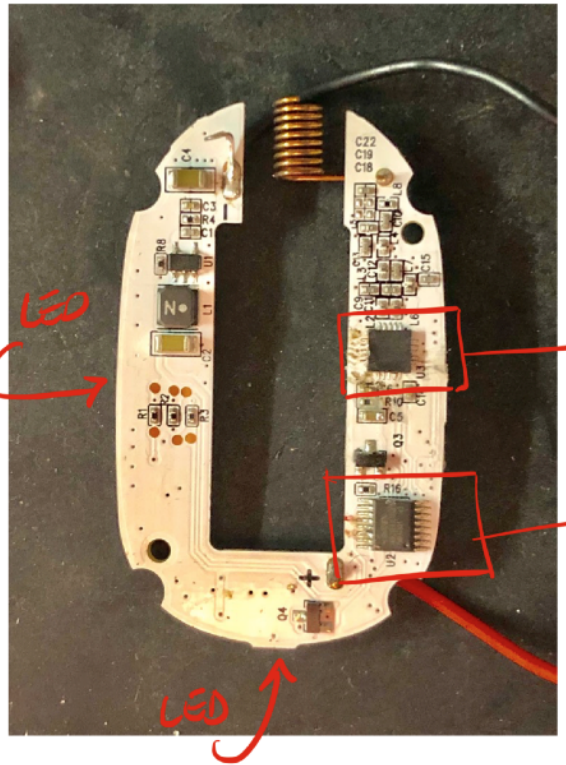
EXTREMA OUTDOOR

PHILIPS

#THIS IS VOYEUR

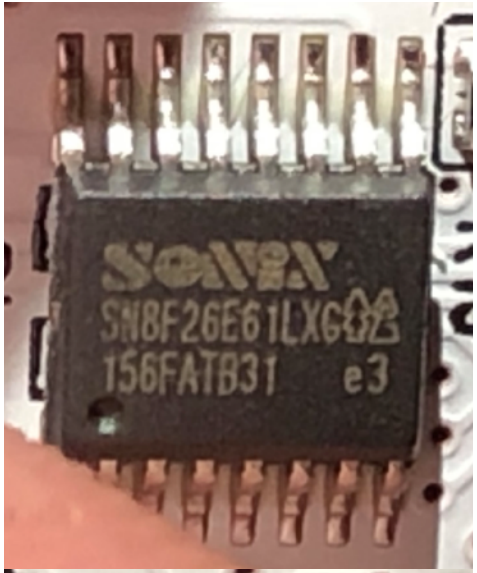
Microsoft

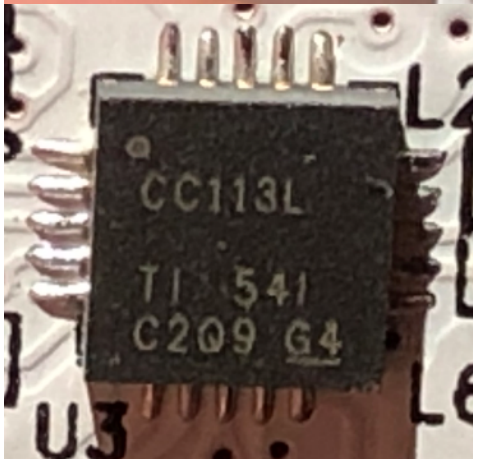
Wanna join the party?

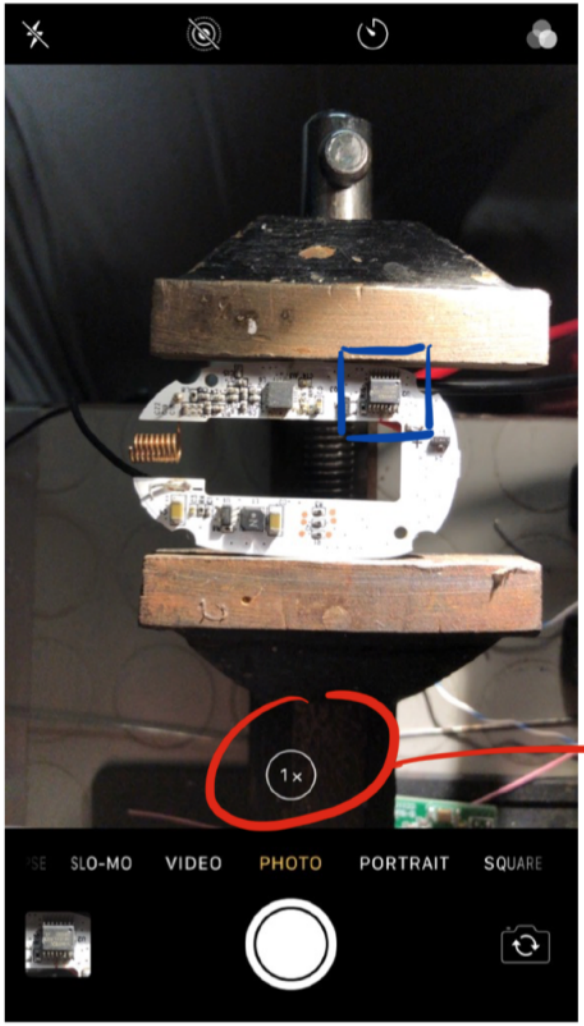


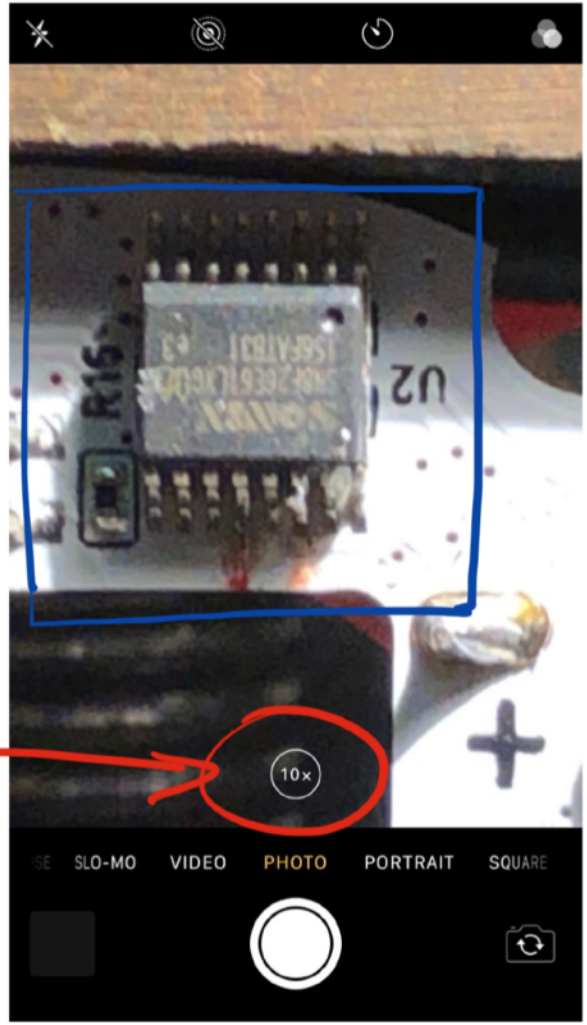
RADIO TRANSCEIVER ? ? ?

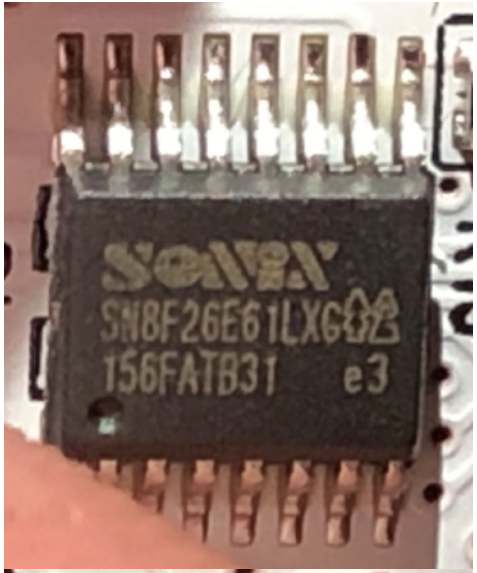
MICRO CONTROLLER ? ? ?


SONIX
SN8F26E61LXG
156FATB31 e3


CC113L
TI 541
C209 G4
U3


1×
SLO-MO
VIDEO
PHOTO
PORTRAIT
SQUARE


R15
U2
10×
SLO-MO
VIDEO
PHOTO
PORTRAIT
SQUARE



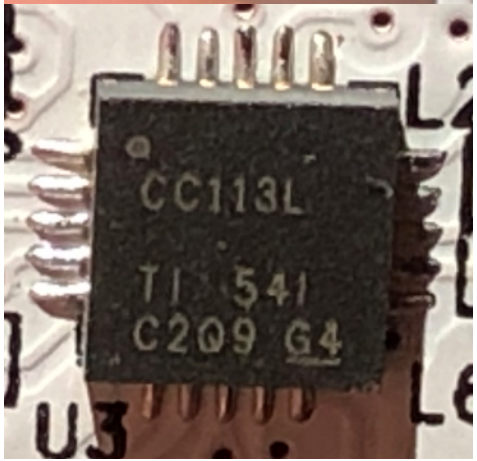
SONIX
SN8F26E61LXG
156FATB31


SONiX

SONiX 8-Bit MCU
INSTRUCTION SET
General Release Specification

SONiX 8-Bit Micro-Controller

SONIX TECHNOLOGY CO., LTD
Revision 1.34



CC113L
TI 541
C2Q9 G4


CC113L Value Line Receiver

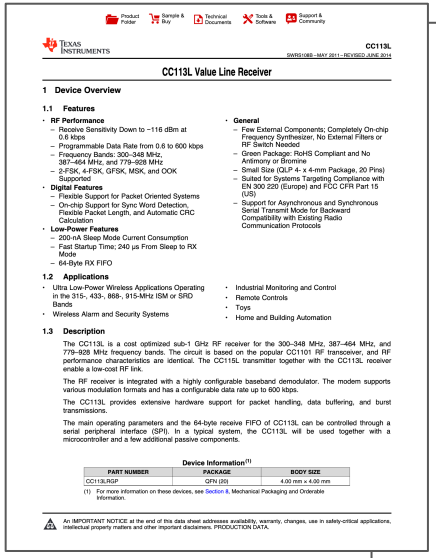
1 Device Overview

1.1 Features

1.2 Applications

1.3 Description

Device Information



Product Folder | Sample & Buy | Technical Documents | Tools & Software | Support & Community

TEXAS INSTRUMENTS

CC113L

SWRS108B – MAY 2011 – REVISED JUNE 2014

CC113L Value Line Receiver

1 Device Overview

1.1 Features

- **RF Performance**
  - Receive Sensitivity Down to −116 dBm at 0.6 kbps
  - Programmable Data Rate from 0.6 to 600 kbps
  - Frequency Bands: 300–348 MHz, 387–464 MHz, and 779–928 MHz
  - 2-FSK, 4-FSK, GFSK, MSK, and OOK Supported
- **Digital Features**
  - Flexible Support for Packet Oriented Systems
  - On-chip Support for Sync Word Detection, Flexible Packet Length, and Automatic CRC Calculation
- **Low-Power Features**
  - 200-nA Sleep Mode Current Consumption
  - Fast Startup Time; 240 µs From Sleep to RX Mode
  - 64-Byte RX FIFO
- **General**
  - Few External Components; Completely On-chip Frequency Synthesizer, No External Filters or RF Switch Needed
  - Green Package: RoHS Compliant and No Antimony or Bromine
  - Small Size (QLP 4- x 4-mm Package, 20 Pins)
  - Suited for Systems Targeting Compliance with EN 300 220 (Europe) and FCC CFR Part 15 (US)
  - Support for Asynchronous and Synchronous Serial Transmit Mode for Backward Compatibility with Existing Radio Communication Protocols

1.2 Applications

- Ultra Low-Power Wireless Applications Operating in the 315-, 433-, 868-, 915-MHz ISM or SRD Bands
- Wireless Alarm and Security Systems
- Industrial Monitoring and Control
- Remote Controls
- Toys
- Home and Building Automation

1.3 Description

The CC113L is a cost optimized sub-1 GHz RF receiver for the 300–348 MHz, 387–464 MHz, and 779–928 MHz frequency bands. The circuit is based on the popular CC1101 RF transceiver, and RF performance characteristics are identical. The CC115L transmitter together with the CC113L receiver enable a low-cost RF link.

The RF receiver is integrated with a highly configurable baseband demodulator. The modem supports various modulation formats and has a configurable data rate up to 600 kbps.

The CC113L provides extensive hardware support for packet handling, data buffering, and burst transmissions.

The main operating parameters and the 64-byte receive FIFO of CC113L can be controlled through a serial peripheral interface (SPI). In a typical system, the CC113L will be used together with a microcontroller and a few additional passive components.

Device Information(1)

PART NUMBER	PACKAGE	BODY SIZE
CC113LRGP	QFN (20)	4.00 mm × 4.00 mm

(1) For more information on these devices, see Section 8, Mechanical Packaging and Orderable Information.

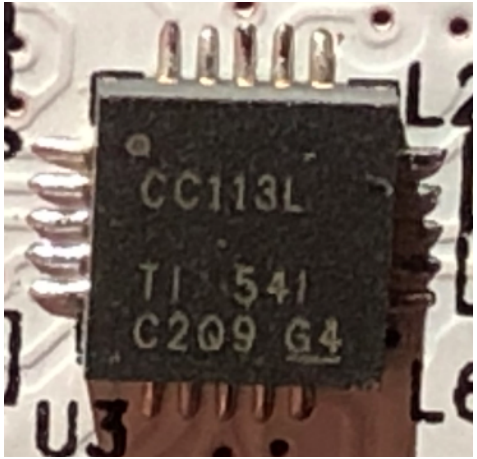
An IMPORTANT NOTICE at the end of this data sheet addresses availability, warranty, changes, use in safety-critical applications, intellectual property matters and other important disclaimers. PRODUCTION DATA.

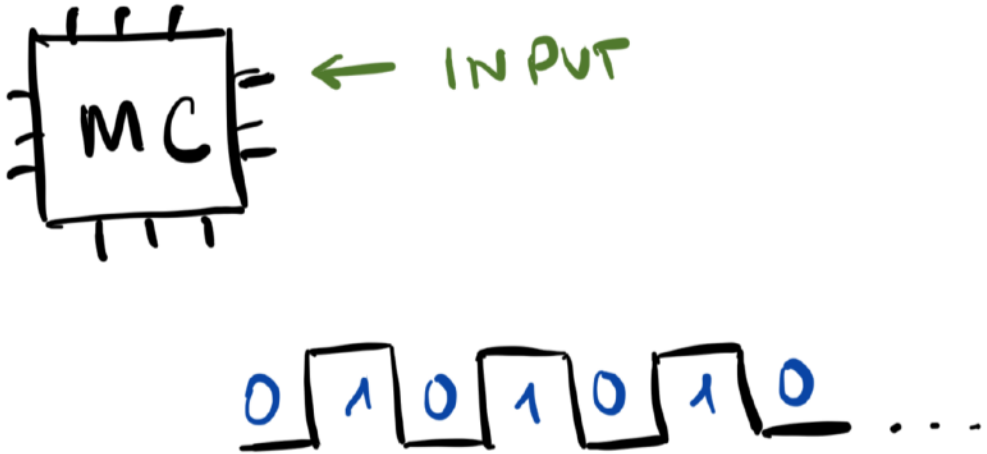
1.1 Features

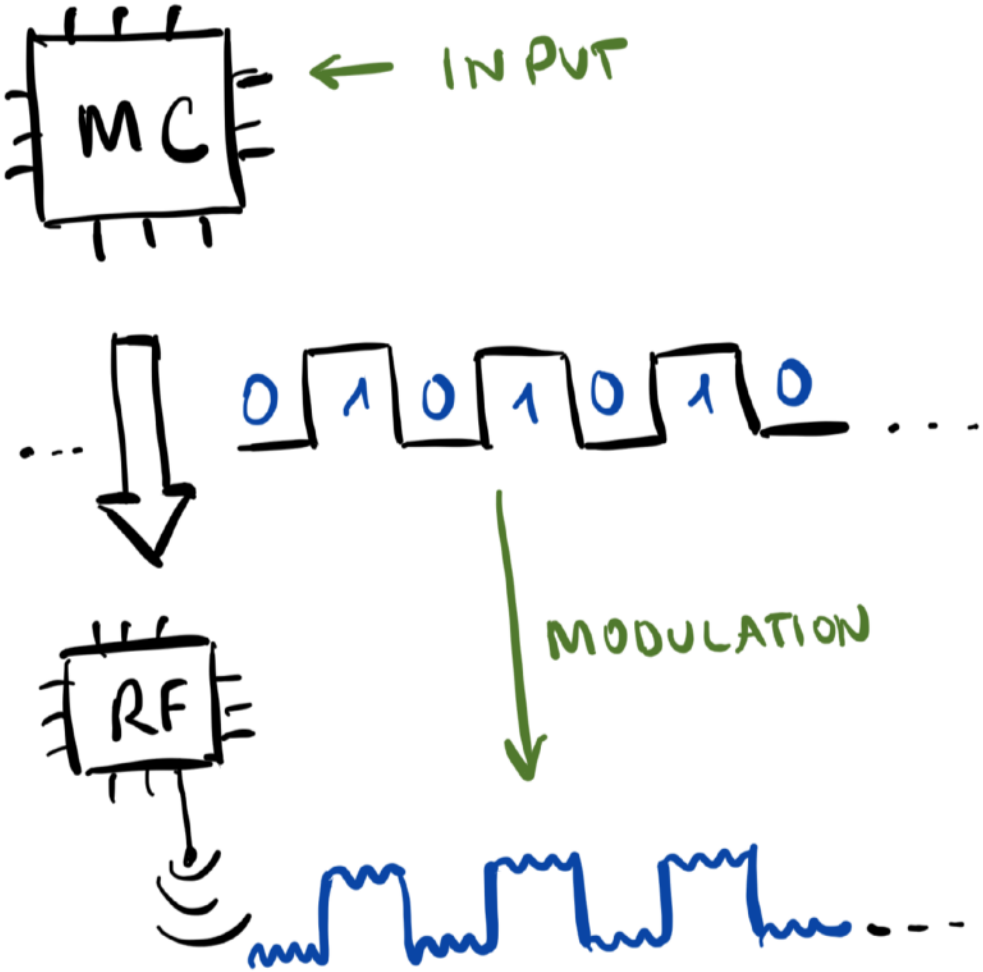
- **RF Performance**
  - Receive Sensitivity Down to −116 dBm at 0.6 kbps
  - Programmable Data Rate from 0.6 to 600 kbps
  - Frequency Bands: 300–348 MHz, 387–464 MHz, and 779–928 MHz
  - 2-FSK, 4-FSK, GFSK, MSK, and OOK Supported
- **Digital Features**
  - Flexible Support for Packet Oriented Systems
  - On-chip Support for Sync Word Detection, Flexible Packet Length, and Automatic CRC Calculation
- **Low-Power Features**
  - 200-nA Sleep Mode Current Consumption
  - Fast Startup Time; 240 µs From Sleep to RX Mode
  - 64-Byte RX FIFO

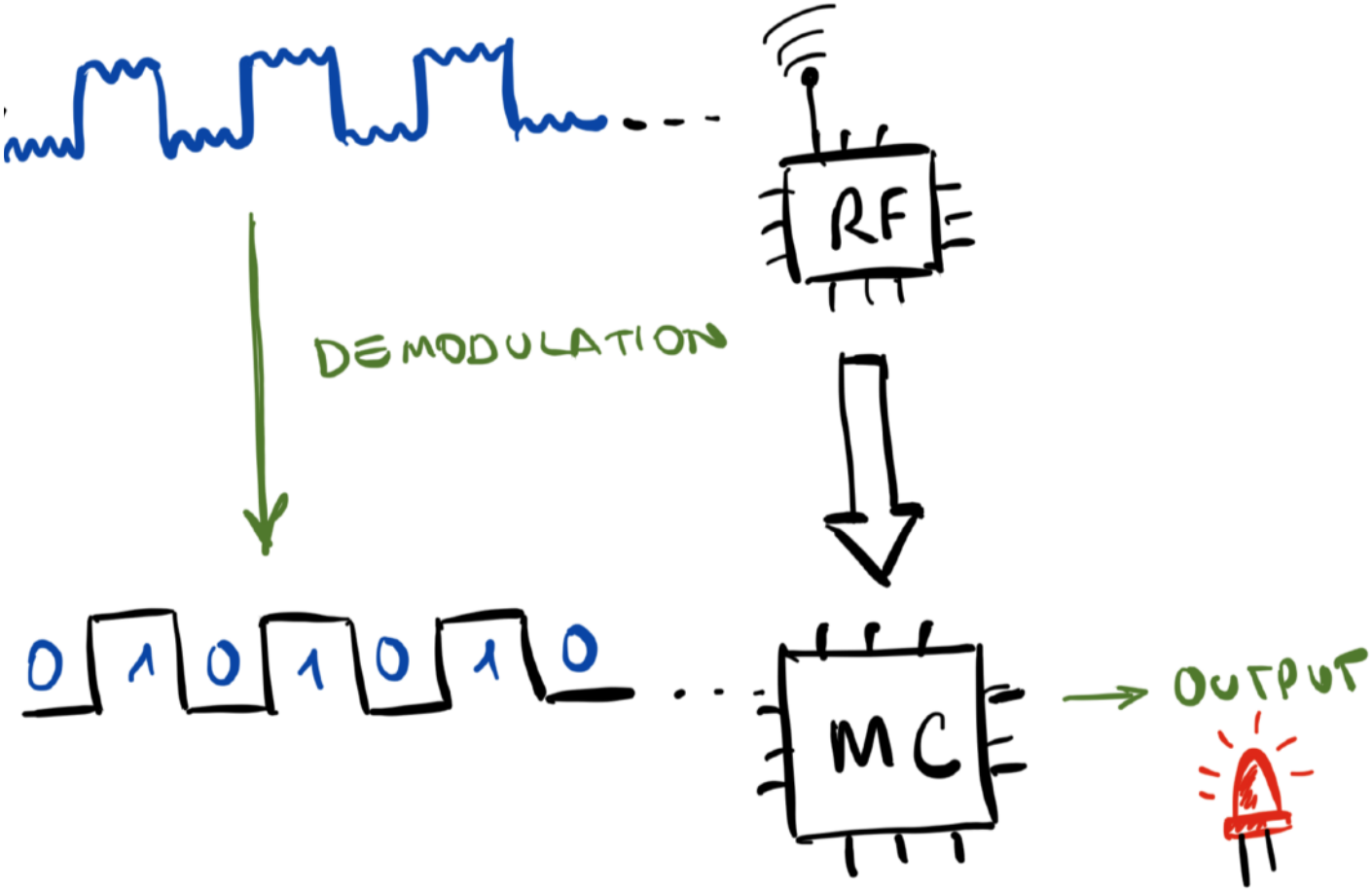
1.2 Applications

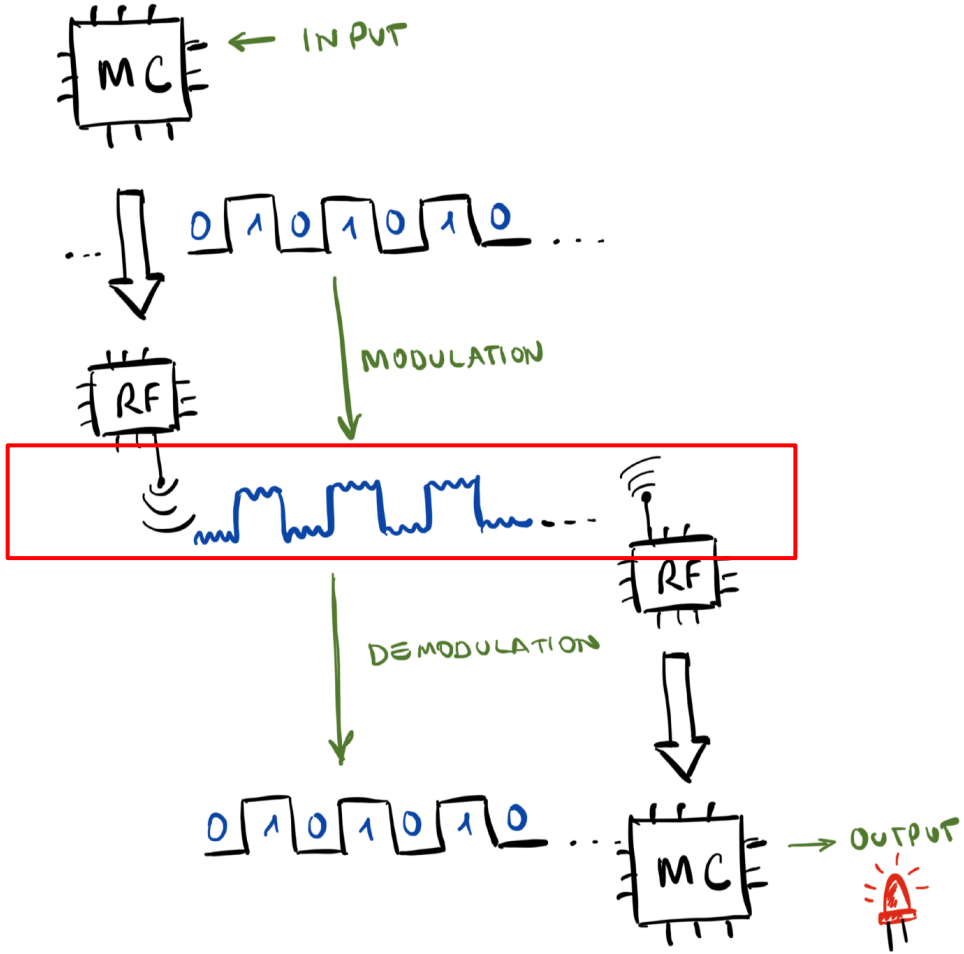
- Ultra Low-Power Wireless Applications Operating in the 315-, 433-, 868-, 915-MHz ISM or SRD Bands
- Wireless Alarm and Security Systems

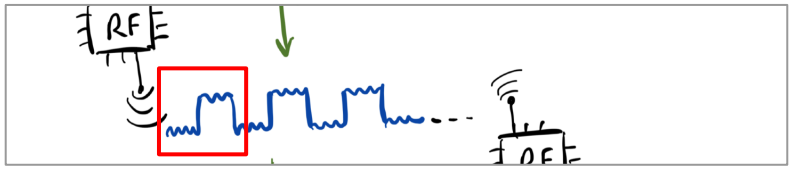


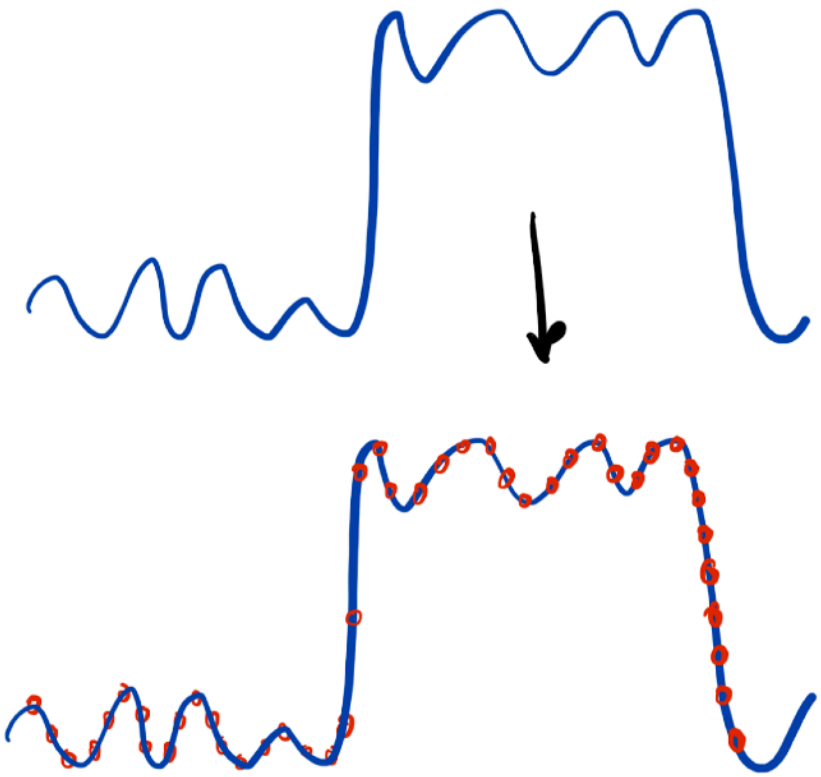


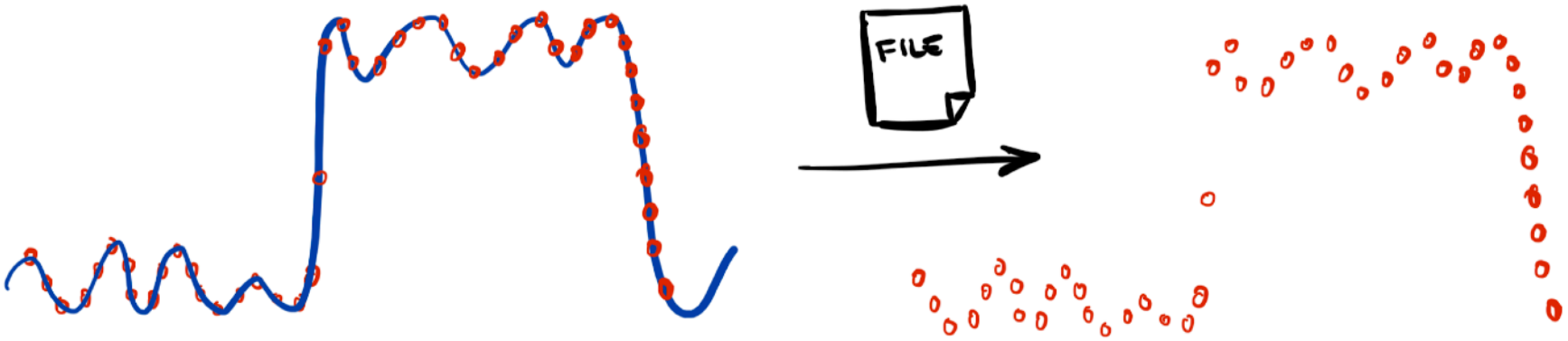




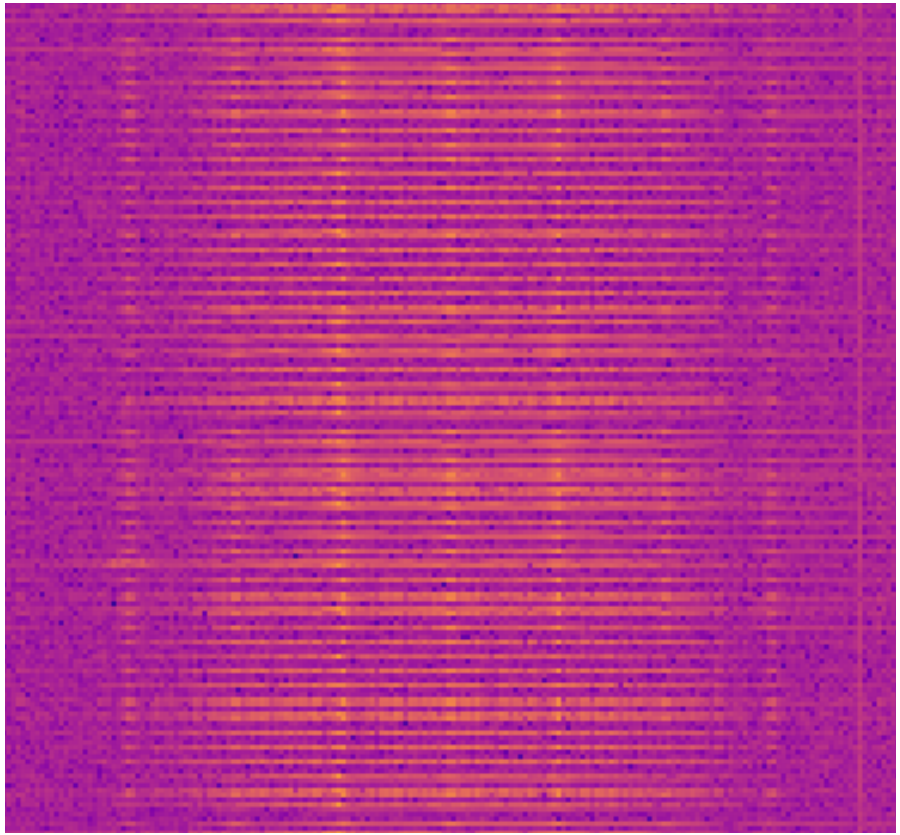


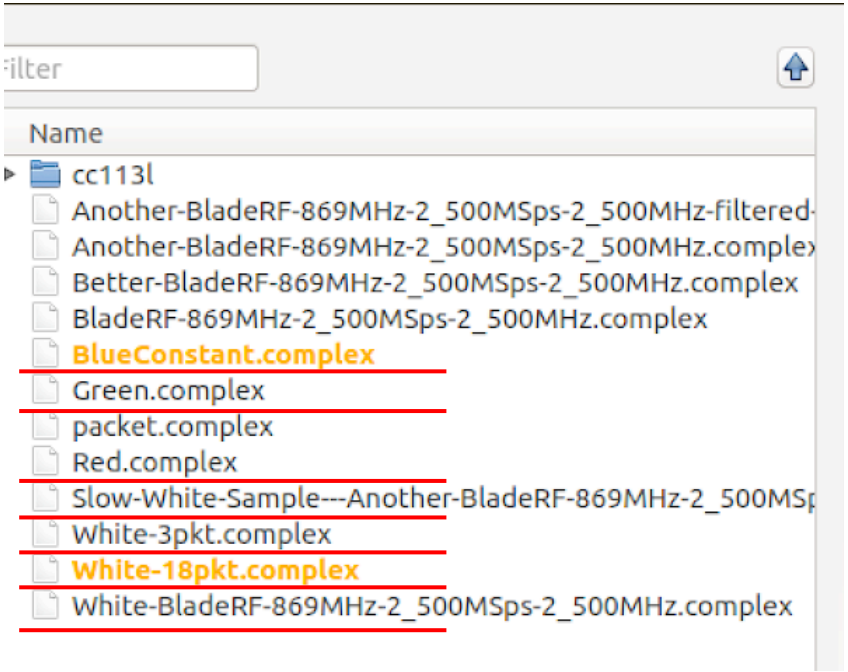


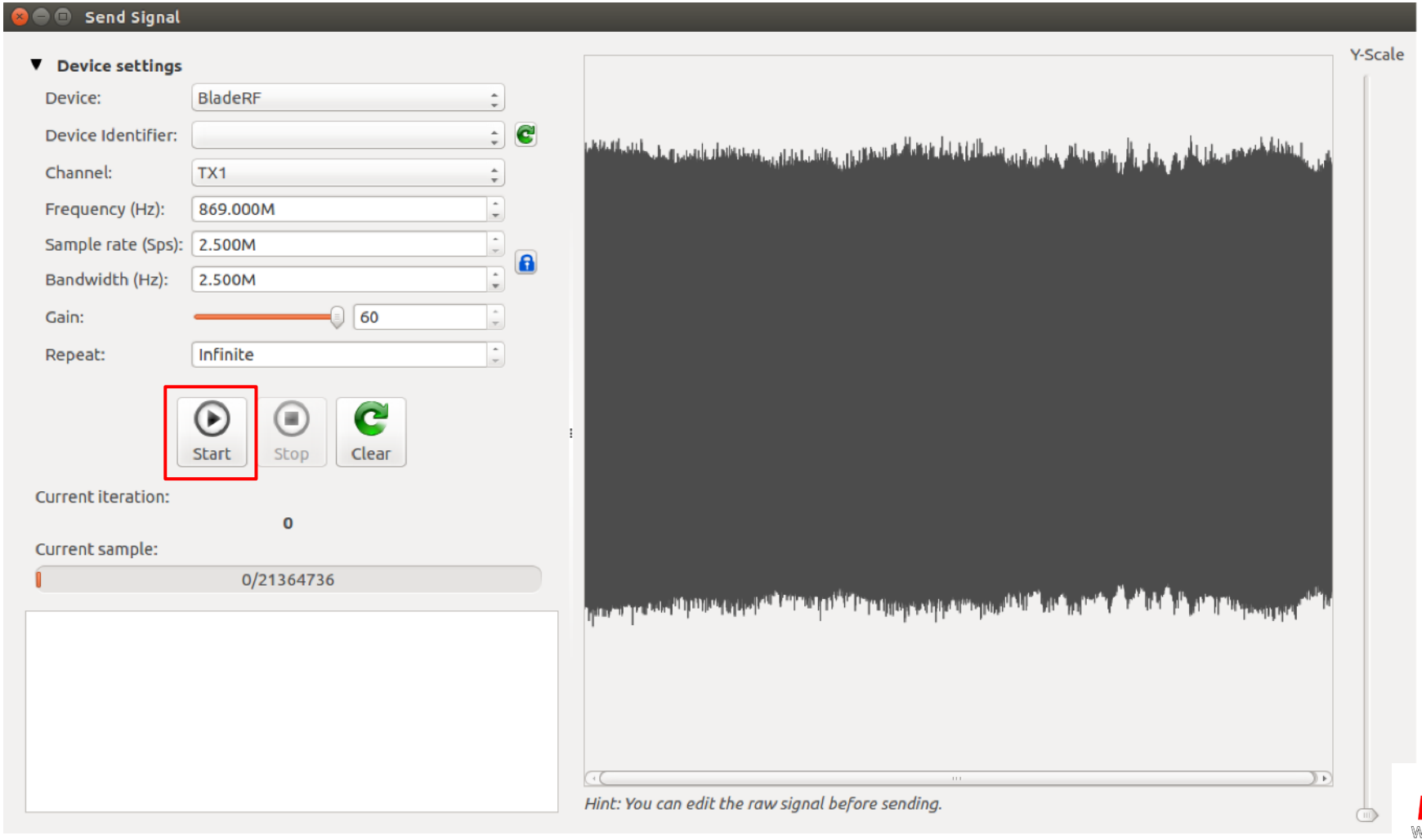



FILE


2:00AM






Send Signal
Device settings
Device:
BladeRF
Device Identifier:
Channel:
TX1
Frequency (Hz):
869.000M
Sample rate (Sps):
2.500M
Bandwidth (Hz):
2.500M
Gain:
60
Repeat:
Infinite
Start
Stop
Clear
Current iteration:
0
Current sample:
0/21364736
Y-Scale
Hint: You can edit the raw signal before sending.

DEMO?

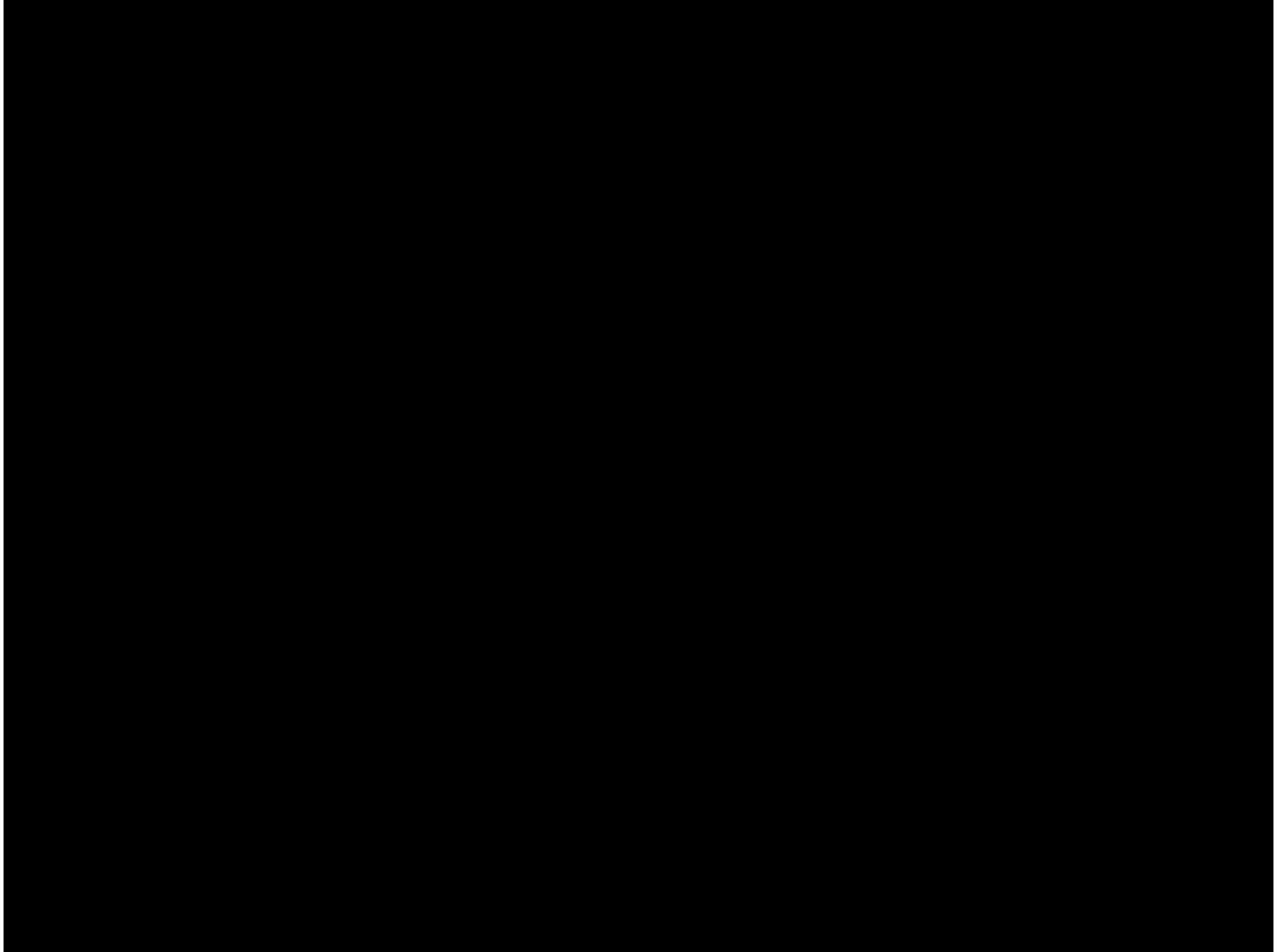










CVE-2018-19023

Hetronic replay-attack vulnerability in radio-frequency industrial remote controllers. More details at ICSA-19-003-03, CVE-2018-19023, and ZDI-19-003.

ZDI-CAN-6183

Autec replay-attack vulnerability in radio-frequency industrial remote controllers. The product under testing has reached end of life and is no longer supported by the vendor. More details.

ZDI-18-1336

Juuko replay-attack vulnerability in radio-frequency industrial remote controllers. More details at ZDI-18-1336.

ZDI-CAN-6185

Circuit Design replay-attack vulnerability in radio-frequency module. More details.

ZDI-18-1362

Juuko arbitrary command injection and remote code execution vulnerability in radio-frequency industrial remote controllers. More details at ZDI-18-1362.

ZDI-CAN-6187

Elca replay-attack vulnerability in radio-frequency industrial remote controllers. The product under testing has reached end of life and is no longer supported by the vendor. More details.

CVE-2018-17903

Saga replay-attack vulnerability in radio-frequency industrial remote controllers. More details at ICSA-18-296-02, and CVE-2018-17903.

CVE-2018-17921

Saga TX-RX re-pairing without human interaction in radio-frequency industrial radio controllers. More details at ICSA-18-296-02, and CVE-2018-17921.

CVE-2018-17923

Saga unattended reprogramming in radio-frequency industrial radio remote controllers. More details at ICSA-18-296-02, and CVE-2018-17923.

CVE-2018-17935

Telecrane replay-attack vulnerability in radio-frequency industrial radio remote controllers. More details at ICSA-18-296-03, and CVE-2018-17935.

IEC Webstore
International Electrotechnical Commission

HOME SIGN IN HELP CART 0

IEC 62745:2017

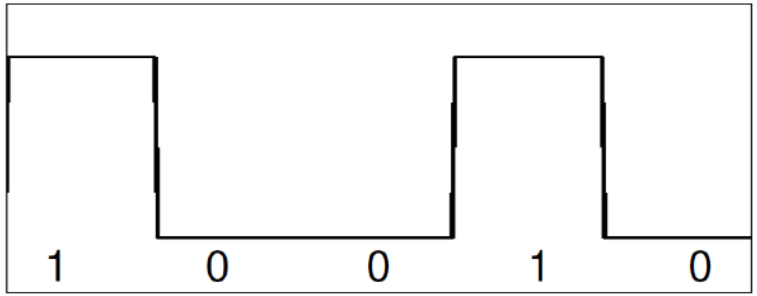
Safety of machinery - Requirements for cableless control systems of machinery

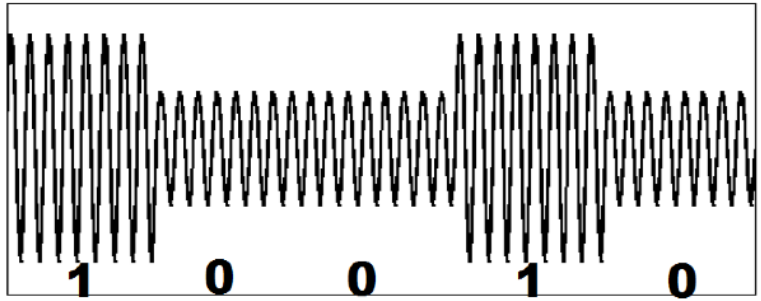
TC 44 | Additional information

Abstract

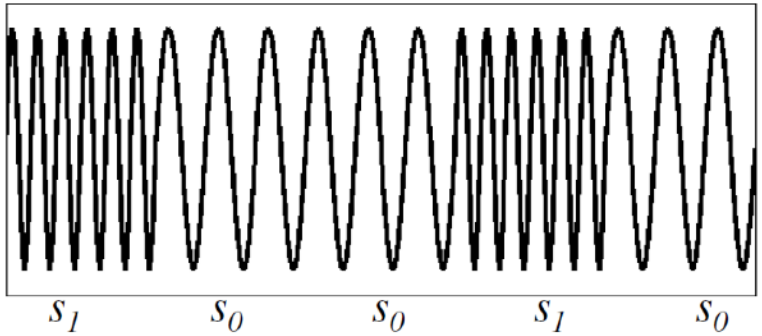
PREVIEW

IEC 62745:2017 specifies requirements for the functionality and interfacing of cableless (for example, radio, infra-red) control systems that provide communication between operator control station(s) and the control system of a machine. Specific requirements are included for such operator control stations that are portable by the operator.

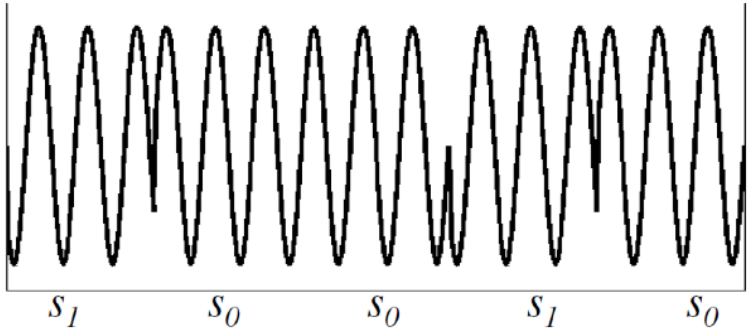




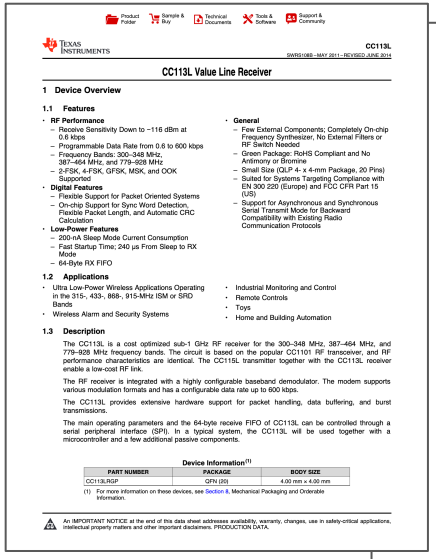
AMPIEZZA



FREQUENZA



FASE



Product Folder | Sample & Buy | Technical Documents | Tools & Software | Support & Community

TEXAS INSTRUMENTS

CC113L

SWRS108B – MAY 2011 – REVISED JUNE 2014

CC113L Value Line Receiver

1 Device Overview

1.1 Features

- **RF Performance**
  - Receive Sensitivity Down to −116 dBm at 0.6 kbps
  - Programmable Data Rate from 0.6 to 600 kbps
  - Frequency Bands: 300–348 MHz, 387–464 MHz, and 779–928 MHz
  - 2-FSK, 4-FSK, GFSK, MSK, and OOK Supported
- **Digital Features**
  - Flexible Support for Packet Oriented Systems
  - On-chip Support for Sync Word Detection, Flexible Packet Length, and Automatic CRC Calculation
- **Low-Power Features**
  - 200-nA Sleep Mode Current Consumption
  - Fast Startup Time; 240 µs From Sleep to RX Mode
  - 64-Byte RX FIFO
- **General**
  - Few External Components; Completely On-chip Frequency Synthesizer, No External Filters or RF Switch Needed
  - Green Package: RoHS Compliant and No Antimony or Bromine
  - Small Size (QLP 4- x 4-mm Package, 20 Pins)
  - Suited for Systems Targeting Compliance with EN 300 220 (Europe) and FCC CFR Part 15 (US)
  - Support for Asynchronous and Synchronous Serial Transmit Mode for Backward Compatibility with Existing Radio Communication Protocols

1.2 Applications

- Ultra Low-Power Wireless Applications Operating in the 315-, 433-, 868-, 915-MHz ISM or SRD Bands
- Wireless Alarm and Security Systems
- Industrial Monitoring and Control
- Remote Controls
- Toys
- Home and Building Automation

1.3 Description

The CC113L is a cost optimized sub-1 GHz RF receiver for the 300–348 MHz, 387–464 MHz, and 779–928 MHz frequency bands. The circuit is based on the popular CC1101 RF transceiver, and RF performance characteristics are identical. The CC115L transmitter together with the CC113L receiver enable a low-cost RF link.

The RF receiver is integrated with a highly configurable baseband demodulator. The modem supports various modulation formats and has a configurable data rate up to 600 kbps.

The CC113L provides extensive hardware support for packet handling, data buffering, and burst transmissions.

The main operating parameters and the 64-byte receive FIFO of CC113L can be controlled through a serial peripheral interface (SPI). In a typical system, the CC113L will be used together with a microcontroller and a few additional passive components.

Device Information(1)

PART NUMBER	PACKAGE	BODY SIZE
CC113LRGP	QFN (20)	4.00 mm × 4.00 mm

(1) For more information on these devices, see Section 8, Mechanical Packaging and Orderable Information.

An IMPORTANT NOTICE at the end of this data sheet addresses availability, warranty, changes, use in safety-critical applications, intellectual property matters and other important disclaimers. PRODUCTION DATA.

1.1 Features

- **RF Performance**
  - Receive Sensitivity Down to −116 dBm at 0.6 kbps
  - Programmable Data Rate from 0.6 to 600 kbps
  - Frequency Bands: 300–348 MHz, 387–464 MHz, and 779–928 MHz
  - 2-FSK, 4-FSK, GFSK, MSK, and OOK Supported
- **Digital Features**
  - Flexible Support for Packet Oriented Systems
  - On-chip Support for Sync Word Detection, Flexible Packet Length, and Automatic CRC Calculation
- **Low-Power Features**
  - 200-nA Sleep Mode Current Consumption
  - Fast Startup Time; 240 µs From Sleep to RX Mode
  - 64-Byte RX FIFO

1.2 Applications

- Ultra Low-Power Wireless Applications Operating in the 315-, 433-, 868-, 915-MHz ISM or SRD Bands
- Wireless Alarm and Security Systems

jopohl / urh

Sponsor | Watch 272 | Star 4,214 | Fork 406

Code | Issues 10 | Pull requests 2 | Wiki | Security | Insights

Universal Radio Hacker: investigate wireless protocols like a boss

security wireless iot sdr hacking hackrf rtl-sdr limesdr usrp dsp sdrplay airspy qt python bladerf radio

Interpretation | Analysis | Gene

1: Complex Signal

White-18pkt

Noise: 0.4858

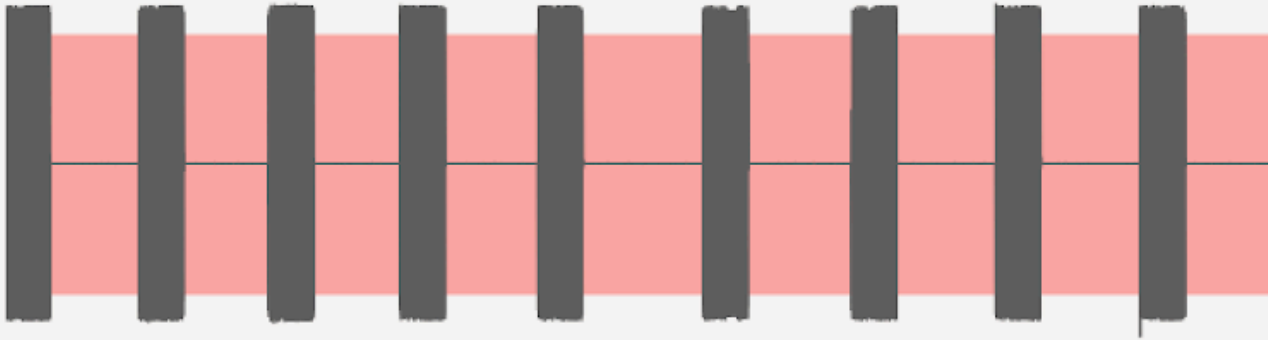
Center: 1.3524

Bit Length: 10

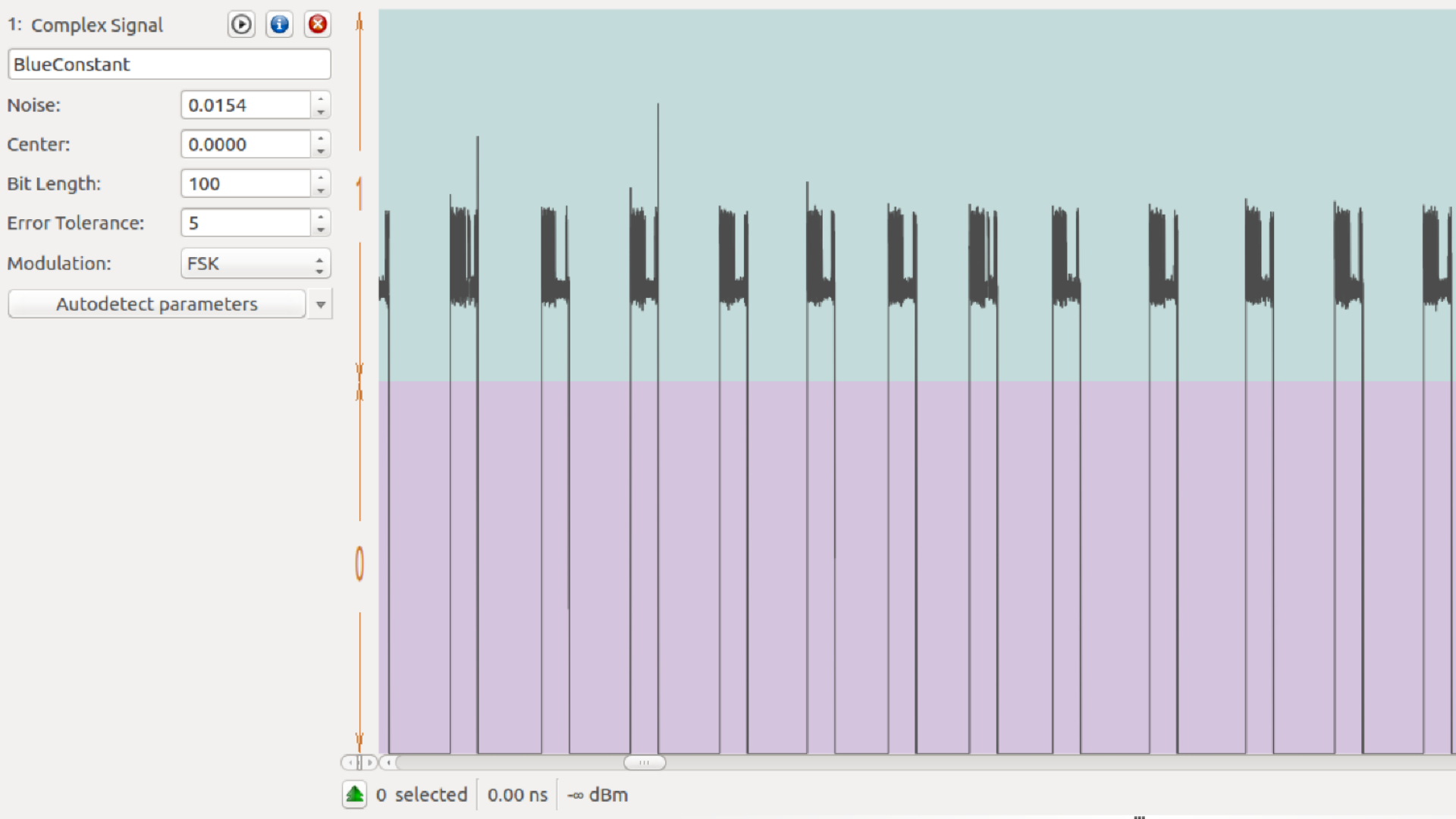
Error Tolerance: 5

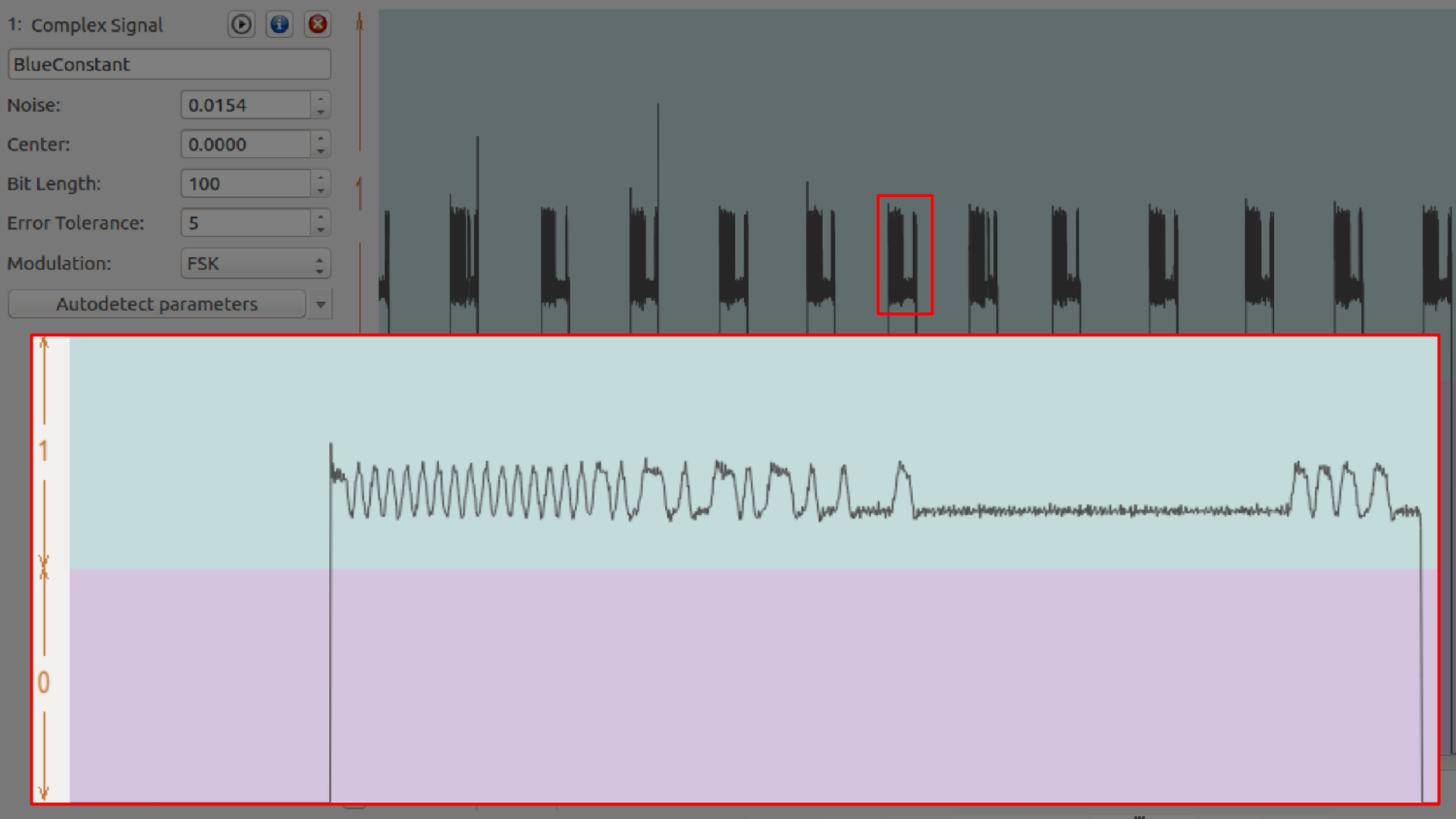
Modulation: FSK

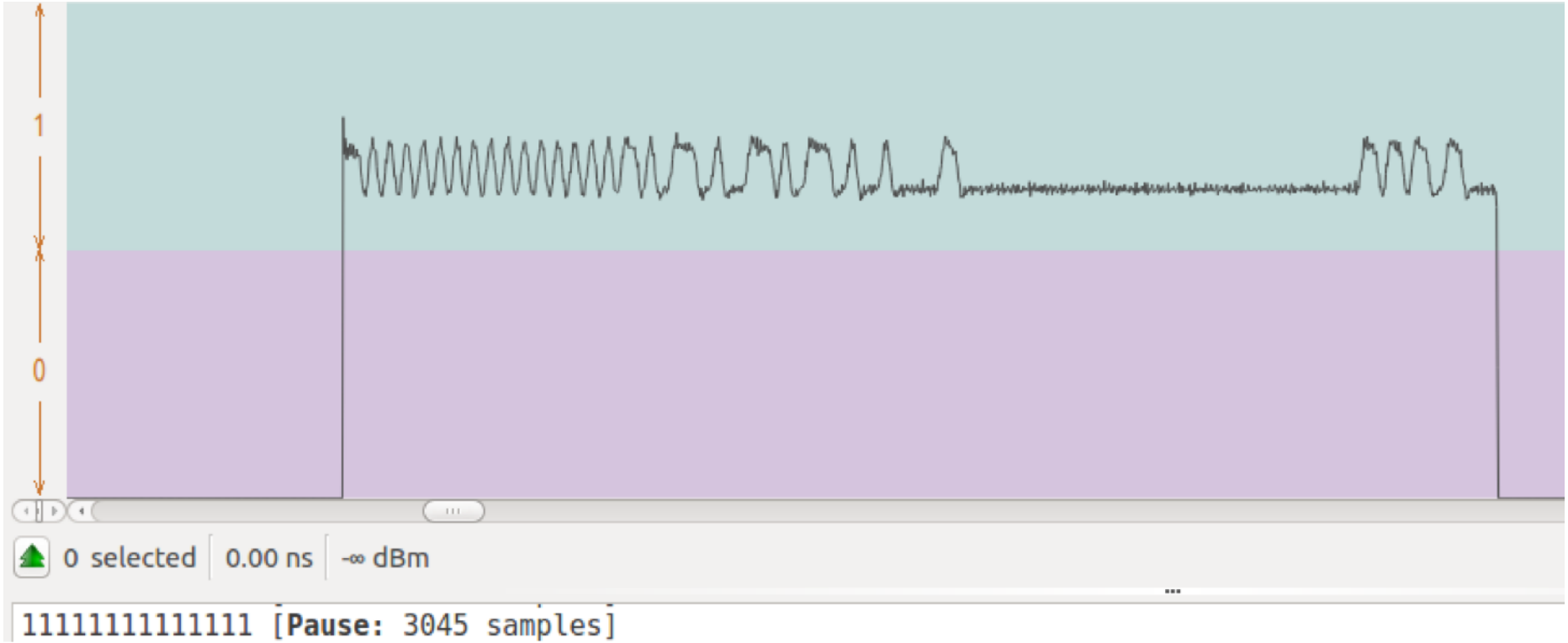
Autodetect parameters

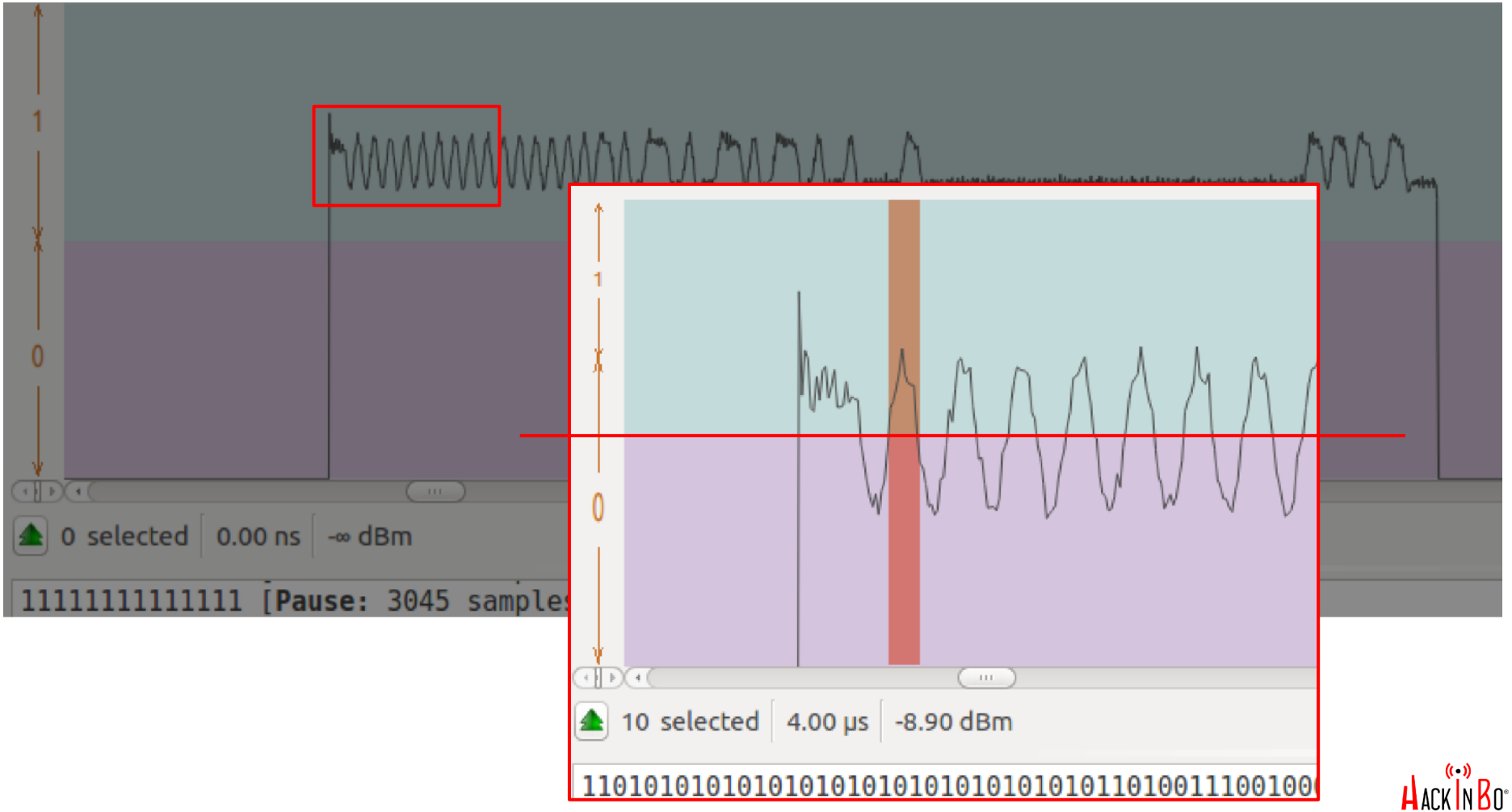


0 selected | 0.00 ns | -∞ dBm


1: Complex Signal
BlueConstant
Noise:
0.0154
Center:
0.0000
Bit Length:
100
Error Tolerance:
5
Modulation:
FSK
Autodetect parameters
1
0
0 selected
0.00 ns
-∞ dBm

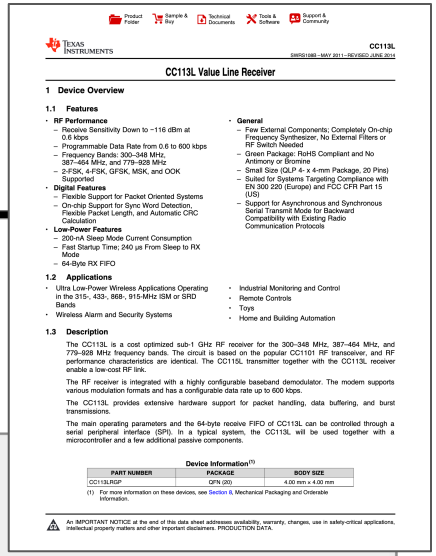

1: Complex Signal
BlueConstant
Noise:
0.0154
Center:
0.0000
Bit Length:
100
Error Tolerance:
5
Modulation:
FSK
Autodetect parameters
1
0


1
0
0 selected
0.00 ns
-∞ dBm
11111111111111 [Pause: 3045 samples]



TEXAS INSTRUMENTS

www.ti.com



Product Folder | Sample & Buy | Technical Documents | Tools & Software | Support & Community

TEXAS INSTRUMENTS — CC113L

SWRS108B – MAY 2011 – REVISED JUNE 2014

CC113L Value Line Receiver

1 Device Overview

1.1 Features

- **RF Performance**
  - Receive Sensitivity Down to −116 dBm at 0.6 kbps
  - Programmable Data Rate from 0.6 to 600 kbps
  - Frequency Bands: 300–348 MHz, 387–464 MHz, and 779–928 MHz
  - 2-FSK, 4-FSK, GFSK, MSK, and OOK Supported
- **Digital Features**
  - Flexible Support for Packet Oriented Systems
  - On-chip Support for Sync Word Detection, Flexible Packet Length, and Automatic CRC Calculation
- **Low-Power Features**
  - 200-nA Sleep Mode Current Consumption
  - Fast Startup Time: 240 µs From Sleep to RX Mode
  - 64-Byte RX FIFO
- **General**
  - Few External Components; Completely On-chip Frequency Synthesizer, No External Filters or RF Switch Needed
  - Green Package: RoHS Compliant and No Antimony or Bromine
  - Small Size (QLP 4- x 4-mm Package, 20 Pins)
  - Suited for Systems Targeting Compliance with EN 300 220 (Europe) and FCC CFR Part 15 (US)
  - Support for Asynchronous and Synchronous Serial Transmit Mode for Backward Compatibility with Existing Radio Communication Protocols

1.2 Applications

- Ultra Low-Power Wireless Applications Operating in the 315-, 433-, 868-, 915-MHz ISM or SRD Bands
- Wireless Alarm and Security Systems
- Industrial Monitoring and Control
- Remote Controls
- Toys
- Home and Building Automation

1.3 Description

The CC113L is a cost optimized sub-1 GHz RF receiver for the 300–348 MHz, 387–464 MHz, and 779–928 MHz frequency bands. The circuit is based on the popular CC1101 RF transceiver, and RF performance characteristics are identical. The CC113L transmitter together with the CC113L receiver enable a low-cost RF link.

The RF receiver is integrated with a highly configurable baseband demodulator. The modem supports various modulation formats and has a configurable data rate up to 600 kbps.

The CC113L provides extensive hardware support for packet handling, data buffering, and burst transmissions.

The main operating parameters and the 64-byte receive FIFO of CC113L can be controlled through a serial peripheral interface (SPI). In a typical system, the CC113L will be used together with a microcontroller and a few additional passive components.

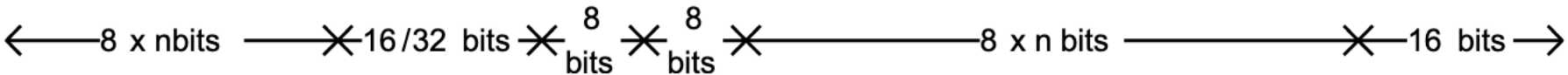
Device Information(1)

PART NUMBER	PACKAGE	BODY SIZE
CC113LRGP	QFN (20)	4.00 mm x 4.00 mm

(1) For more information on these devices, see Section 8, Mechanical Packaging and Orderable Information.

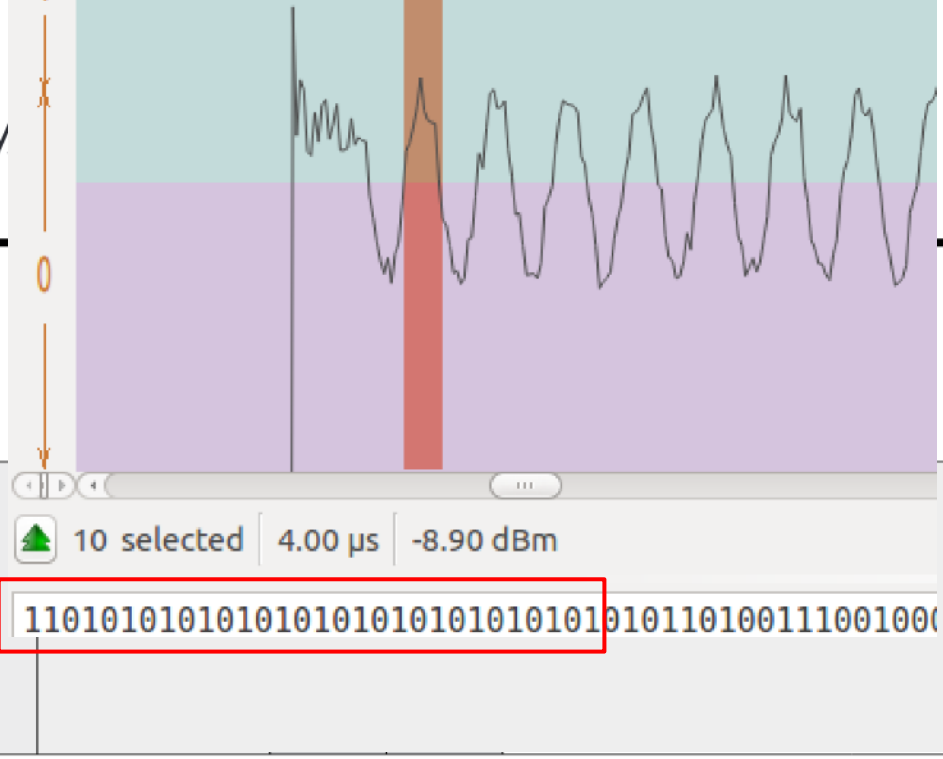
An IMPORTANT NOTICE at the end of this data sheet addresses availability, warranty, changes, use in safety-critical applications, intellectual property matters and other important disclaimers. PRODUCTION DATA.

Preamble bits
(1010...1010)

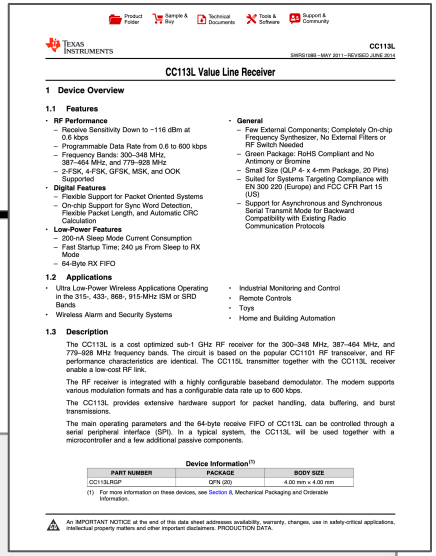


TEXAS INSTRUM

www.ti.com



Preamble bits
(1010...1010)



CC113L Value Line Receiver

1 Device Overview

1.1 Features

- RF Performance
  - Receive Sensitivity Down to −116 dBm at 0.6 kbps
  - Programmable Data Rate from 0.6 to 600 kbps
  - Frequency Bands: 300–348 MHz, 387–464 MHz, and 779–928 MHz
  - 2-FSK, 4-FSK, GFSK, MSK, and OOK Supported
- Digital Features
  - Flexible Support for Packet Oriented Systems
  - On-chip Support for Sync Word Detection, Flexible Packet Length, and Automatic CRC Calculation
- Low-Power Features
  - 200-nA Sleep Mode Current Consumption
  - Fast Startup Time: 240 µs From Sleep to RX Mode
  - 64-Byte RX FIFO
- General
  - Few External Components; Completely On-chip Frequency Synthesizer, No External Filters or RF Switch Needed
  - Green Package: RoHS Compliant and No Antimony or Bromine
  - Small Size (QLP 4- x 4-mm Package, 20 Pins)
  - Suited for Systems Targeting Compliance with EN 300 220 (Europe) and FCC CFR Part 15 (US)
  - Support for Asynchronous and Synchronous Serial Transmit Mode for Backward Compatibility with Existing Radio Communication Protocols

1.2 Applications

- Ultra Low-Power Wireless Applications Operating in the 315-, 433-, 868-, 915-MHz ISM or SRD Bands
- Wireless Alarm and Security Systems
- Industrial Monitoring and Control
- Remote Controls
- Toys
- Home and Building Automation

1.3 Description

The CC113L is a cost optimized sub-1 GHz RF receiver for the 300–348 MHz, 387–464 MHz, and 779–928 MHz frequency bands. The circuit is based on the popular CC1101 RF transceiver, and RF performance characteristics are identical. The CC115L transmitter together with the CC113L receiver enable a low-cost RF link.

The RF receiver is integrated with a highly configurable baseband demodulator. The modem supports various modulation formats and has a configurable data rate up to 600 kbps.

The CC113L provides extensive hardware support for packet handling, data buffering, and burst transmissions.

The main operating parameters and the 64-byte receive FIFO of CC113L can be controlled through a serial peripheral interface (SPI). In a typical system, the CC113L will be used together with a microcontroller and a few additional passive components.

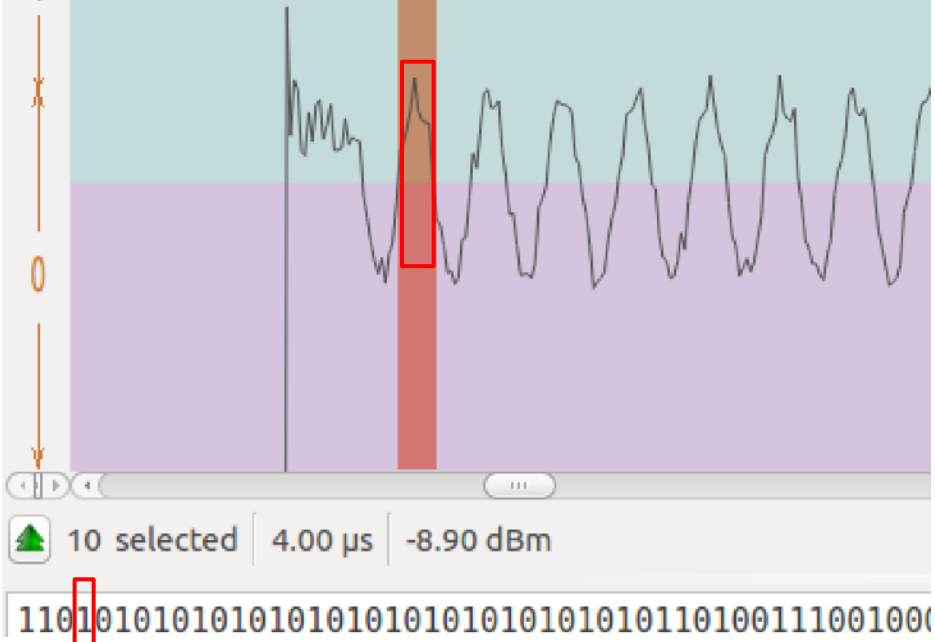
Device Information(1)

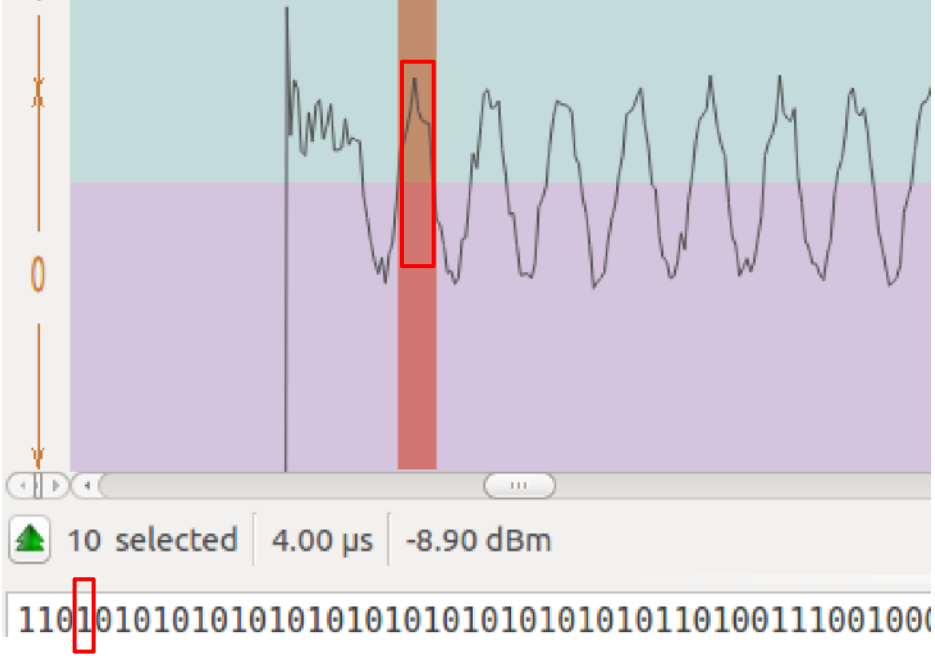
PART NUMBER	PACKAGE	BODY SIZE
CC113LRGP	QFN (20)	4.00 mm x 4.00 mm

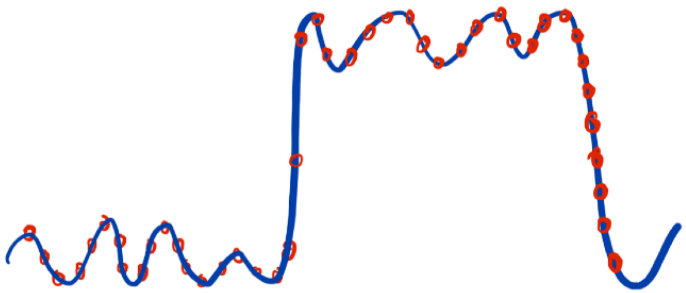
(1) For more information on these devices, see Section 8, Mechanical Packaging and Orderable Information.

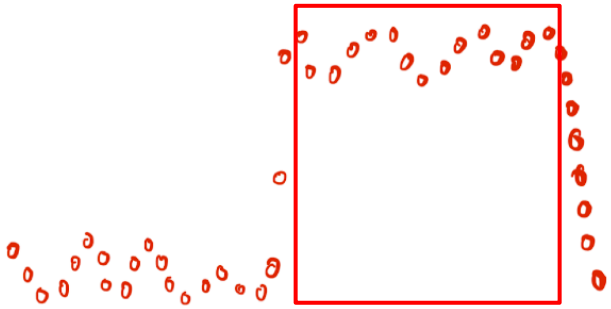
An IMPORTANT NOTICE at the end of this data sheet addresses availability, warranty, changes, use in safety-critical applications, intellectual property matters and other important disclaimers. PRODUCTION DATA.

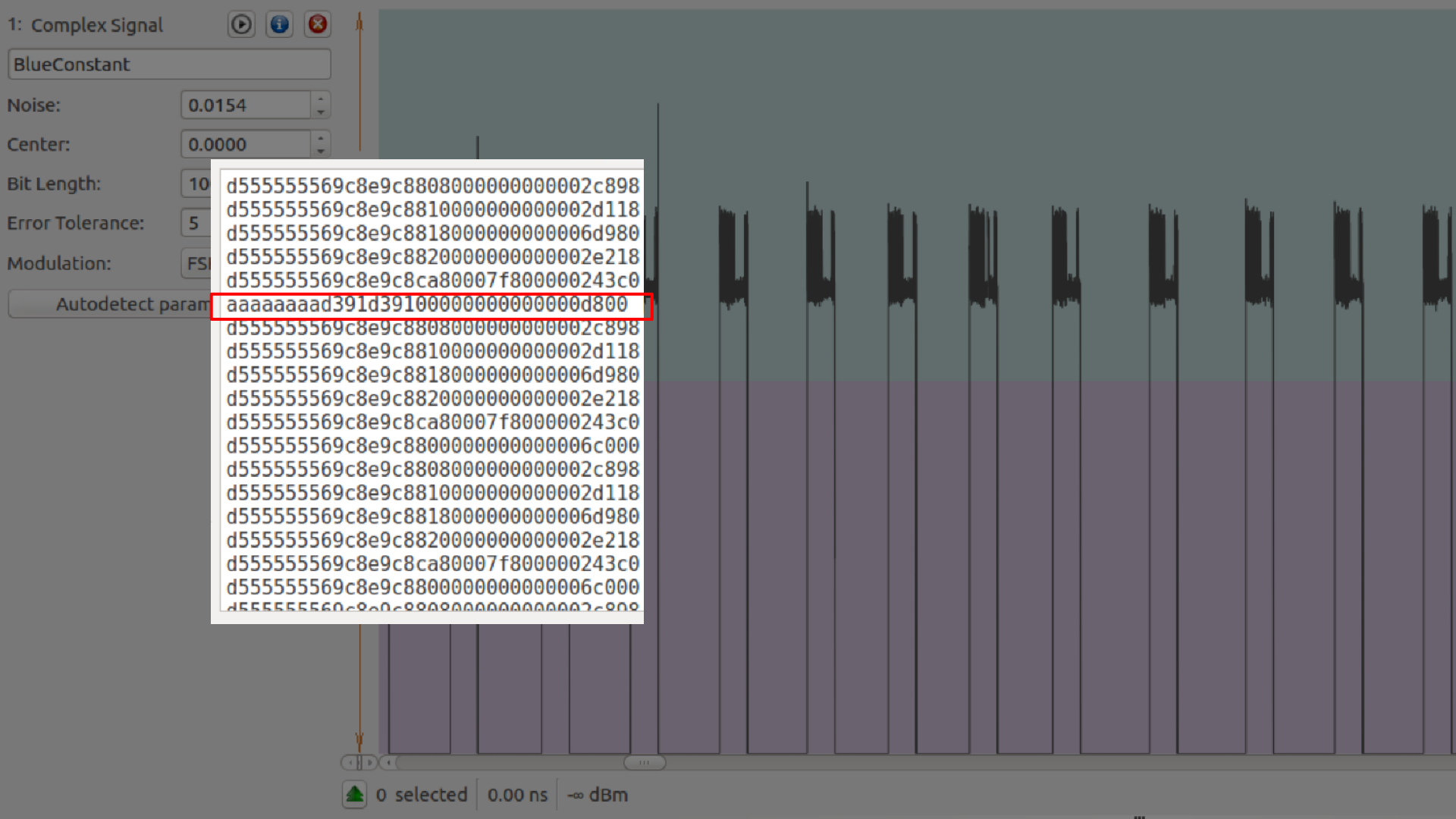
8 x nbits — 16/32 bits — 8 bits — 8 bits — 8 x n bits — 16 bits

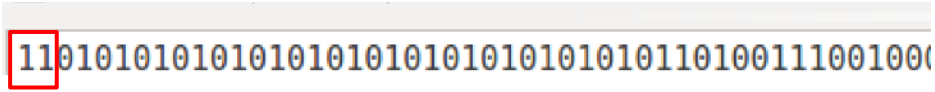


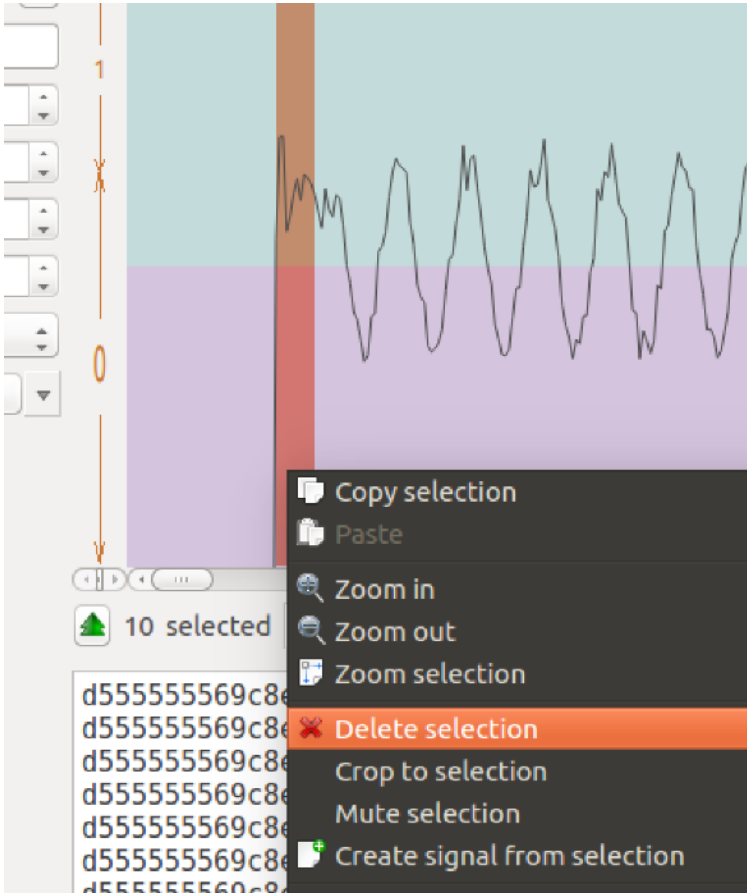

0
10 selected
4.00 µs
-8.90 dBm
11010101010101010101010101010101011010011100100(

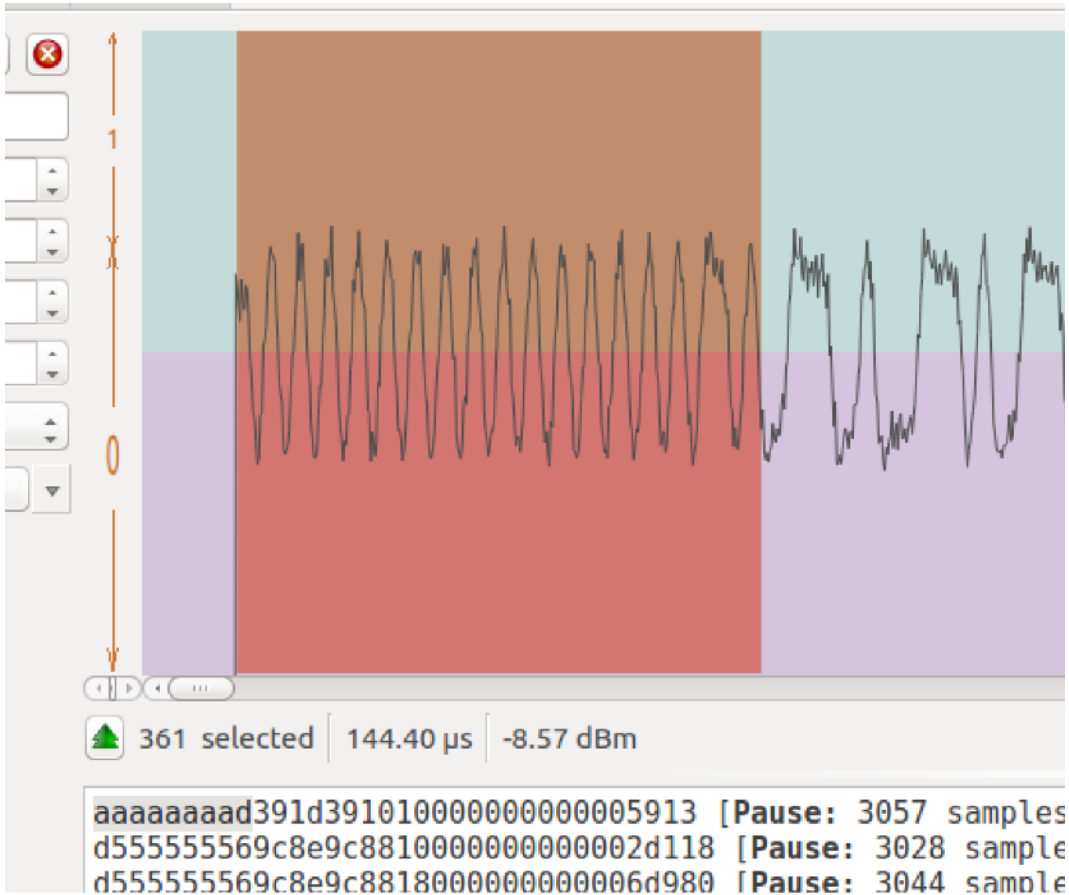





1: Complex Signal
BlueConstant
Noise:
0.0154
Center:
0.0000
Bit Length:
Error Tolerance:
Modulation:
Autodetect param
d555555569c8e9c8808000000000002c898
d555555569c8e9c881000000000002d118
d555555569c8e9c8818000000000006d980
d555555569c8e9c882000000000002e218
d555555569c8e9c8ca80007f800000243c0
aaaaaaaad391d39100000000000000d800
d555555569c8e9c8808000000000002c898
d555555569c8e9c881000000000002d118
d555555569c8e9c8818000000000006d980
d555555569c8e9c882000000000002e218
d555555569c8e9c8ca80007f800000243c0
d555555569c8e9c8800000000000006c000
d555555569c8e9c8808000000000002c898
d555555569c8e9c881000000000002d118
d555555569c8e9c8818000000000006d980
d555555569c8e9c882000000000002e218
d555555569c8e9c8ca80007f800000243c0
d555555569c8e9c8800000000000006c000
0 selected
0.00 ns
-∞ dBm

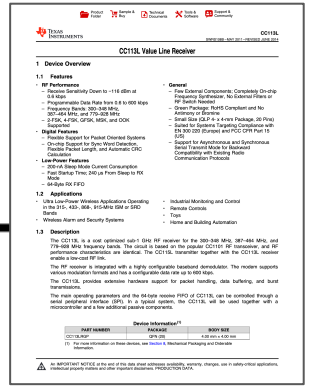



1
0
Copy selection
Paste
Zoom in
Zoom out
Zoom selection
Delete selection
Crop to selection
Mute selection
Create signal from selection
10 selected
d555555569c8e
d555555569c8e
d555555569c8e
d555555569c8e
d555555569c8e
d555555569c8e


1
0
361 selected
144.40 µs
-8.57 dBm
aaaaaaaad391d391010000000000005913 [Pause: 3057 samples
d555555569c8e9c8810000000000002d118 [Pause: 3028 sample
d555555569c8e9c8818000000000006d980 [Pause: 3044 sample

TEXAS INSTRUMENTS

www.ti.com



CC113L Value Line Receiver

1 Device Overview

1.1 Features

- RF Performance
  - High Sensitivity Down to −116 dBm at 0.6 kbps
  - Programmable Data Rate from 0.6 to 600 kbps
  - Frequency Bands: 300–348 MHz, 387–464 MHz, and 779–928 MHz
  - 2-FSK, 4-FSK, GFSK, MSK, and OOK Supported
- Digital Features
  - Flexible Support for Packet Oriented Systems
  - On-chip Support for Sync Word Detection, Flexible Packet Length, and Automatic CRC Handling
- Low-Power Features
  - 200-nA Sleep Mode Current Consumption
  - Fast Startup Time: 240 µs From Sleep to RX Mode
  - 64-Byte RX FIFO
- General
  - Few External Components: Completely On-chip Frequency Synthesizer, No External Filters or RF Switch Needed
  - Green Packages: RoHS Compliant and No Antimony or Bromine
  - Small Size: QFN 4 × 4-mm Package, 20 Pins)
  - Suited for Systems Targeting Compliance with EN 300 220 (Europe) and FCC CFR Part 15 (US)
  - Support for Asynchronous and Synchronous Serial Receive Mode for Backward Compatibility with Existing Radio Communication Protocols

1.2 Applications

- Ultra Low-Power Wireless Applications Operating in the 315-, 433-, 868-, 915-MHz ISM or SRD Bands
- Wireless Alarm and Security Systems
- Industrial Monitoring and Control
- Remote Controls
- Toys
- Home and Building Automation

1.3 Description

The CC113L is a cost optimized sub-1 GHz RF receiver for the 300–348 MHz, 387–464 MHz, and 779–928 MHz frequency bands. The circuit is based on the popular CC1101 RF transceiver, and RF performance characteristics are identical. The CC113L transmitter together with the CC113L receiver enable a low-cost RF link.

The RF receiver is integrated with a highly configurable baseband demodulator. The modem supports various modulation formats and has a configurable data rate up to 600 kbps.

The CC113L provides extensive hardware support for packet handling, data buffering, and burst transmissions.

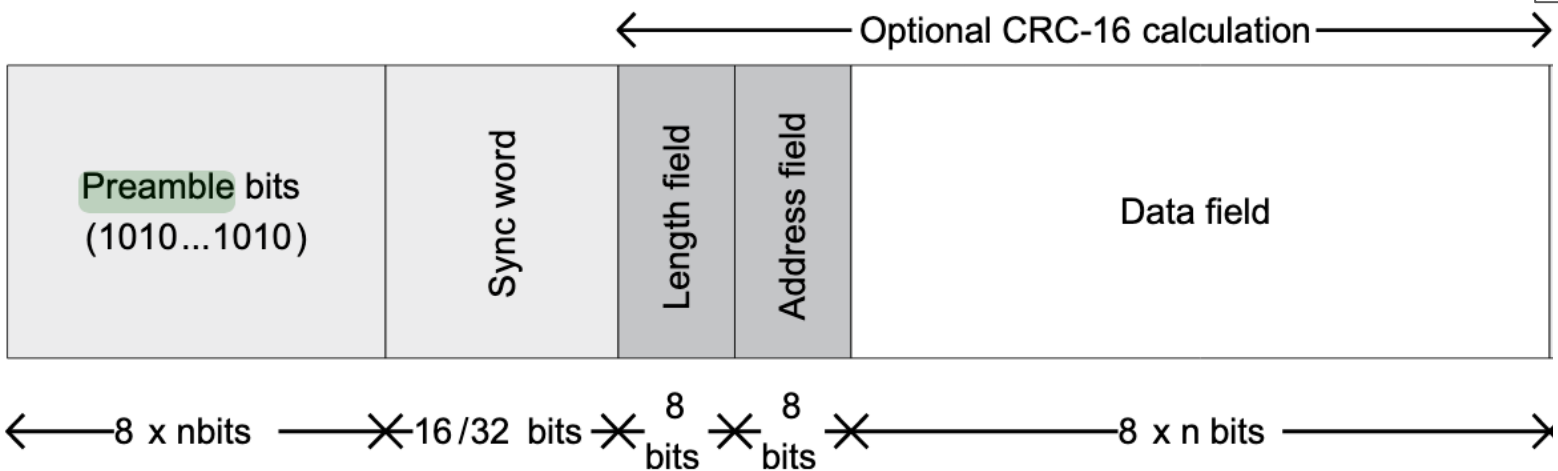
The main operating parameters and the 64-byte receive FIFO of CC113L can be controlled through a serial peripheral interface (SPI). In a typical system, the CC113L will be used together with a microcontroller and a few additional passive components.

Device Information[1][2]

PART NUMBER	PACKAGE	BODY SIZE
CC113LRGP	QFN 20E	4.00 mm × 4.00 mm

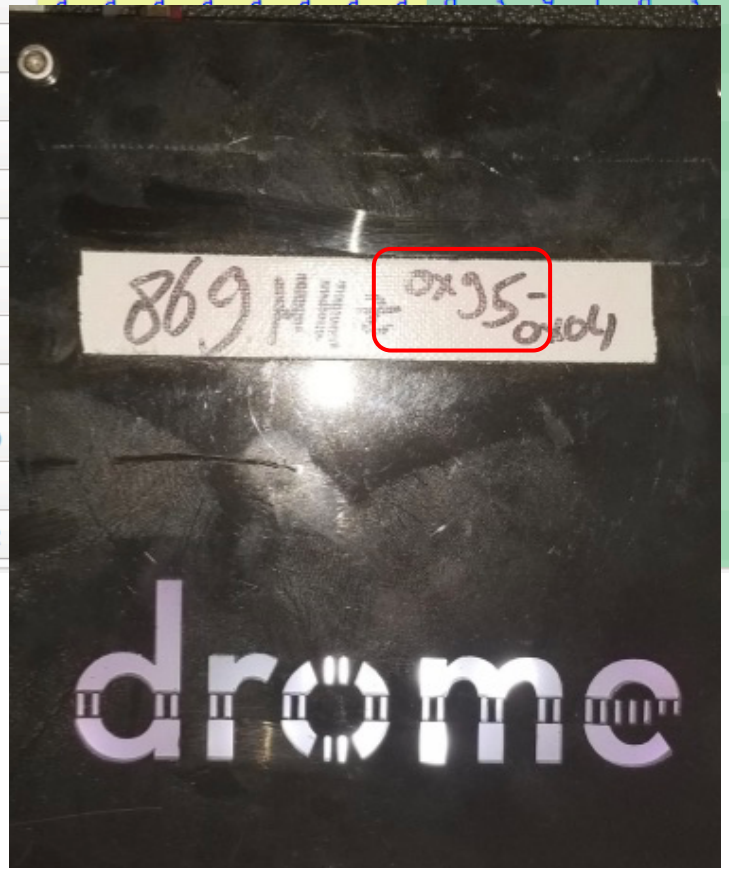
(1) For more information on these devices, see Section 8, Mechanical Packaging and Orderable Information.

An IMPORTANT NOTICE at the end of this data sheet addresses availability, warranty, changes, use in safety-critical applications, intellectual property matters and other important disclaimers. PRODUCTION DATA.



	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
1	a	a	a	a	a	a	a	a	d	3	9	1	d	3	9	1	0	1	0	0	0	0	0	0
2	a	a	a	a	a	a	a	a	d	3	9	1	d	3	9	1	0	2	0	0	0	0	0	0
3	a	a	a	a	a	a	a	a	d	3	9	1	d	3	9	1	0	3	0	0	0	0	0	0
4	a	a	a	a	a	a	a	a	d	3	9	1	d	3	9	1	0	4	0	0	0	0	0	0
5	a	a	a	a	a	a	a	a	d	3	9	1	d	3	9	1	9	5	0	0	0	0	F	F
6	a	a	a	a	a	a	a	a	d	3	9	1	d	3	9	1	0	0	0	0	0	0	0	0
7	a	a	a	a	a	a	a	a	d	3	9	1	d	3	9	1	0	1	0	0	0	0	0	0
8	a	a	a	a	a	a	a	a	d	3	9	1	d	3	9	1	0	2	0	0	0	0	0	0
9	a	a	a	a	a	a	a	a	d	3	9	1	d	3	9	1	0	3	0	0	0	0	0	0
10	a	a	a	a	a	a	a	a	d	3	9	1	d	3	9	1	0	4	0	0	0	0	0	0
11	a	a	a	a	a	a	a	a	d	3	9	1	d	3	9	1	9	5	0	0	0	0	F	F
12	a	a	a	a	a	a	a	a	d	3	9	1	d	3	9	1	0	0	0	0	0	0	0	0

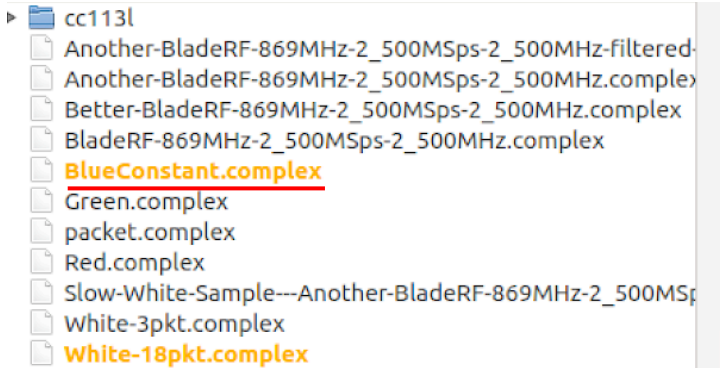
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
1	a	a	a	a	a	a	a	a	d	3	9	1	d	3	9	1	0	1	0	0	0	0	0	0
2															9	1	0	2	0	0	0	0	0	0
3															9	1	0	3	0	0	0	0	0	0
4															9	1	0	4	0	0	0	0	0	0
5															9	1	9	5	0	0	0	0	F	F
6															9	1	0	0	0	0	0	0	0	0
7															9	1	0	1	0	0	0	0	0	0
8															9	1	0	2	0	0	0	0	0	0
9															9	1	0	3	0	0	0	0	0	0
10															9	1	0	4	0	0	0	0	0	0
11															9	1	9	5	0	0	0	0	F	F
12															9	1	0	0	0	0	0	0	0	0



	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
1	a	a	a	a	a	a	a	a	d	3	9	1	d	3	9	1	0	1	0	0	0	0	0	0
2	a	a	a	a	a	a	a	a	d	3	9	1	d	3	9	1	0	2	0	0	0	0	0	0
3	a	a	a	a	a	a	a	a	d	3	9	1	d	3	9	1	0	3	0	0	0	0	0	0
4	a	a	a	a	a	a	a	a	d	3	9	1	d	3	9	1	0	4	0	0	0	0	0	0
5	a	a	a	a	a	a	a	a	d	3	9	1	d	3	9	1	9	5	0	0	0	0	F	F
6	a	a	a	a	a	a	a	a	d	3	9	1	d	3	9	1	0	0	0	0	0	0	0	0
7	a	a	a	a	a	a	a	a	d	3	9	1	d	3	9	1	0	1	0	0	0	0	0	0
8	a	a	a	a	a	a	a	a	d	3	9	1	d	3	9	1	0	2	0	0	0	0	0	0
9	a	a	a	a	a	a	a	a	d	3	9	1	d	3	9	1	0	3	0	0	0	0	0	0
10	a	a	a	a	a	a	a	a	d	3	9	1	d	3	9	1	0	4	0	0	0	0	0	0
11	a	a	a	a	a	a	a	a	d	3	9	1	d	3	9	1	9	5	0	0	0	0	F	F
12	a	a	a	a	a	a	a	a	d	3	9	1	d	3	9	1	0	0	0	0	0	0	0	0

#0000FF

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
1	a	a	a	a	a	a	a	a	d	3	9	1	d	3	9	1	0	1	0	0	0	0	0	0
2	a	a	a	a	a	a	a	a	d	3	9	1	d	3	9	1	0	2	0	0	0	0	0	0
3	a	a	a	a	a	a	a	a	d	3	9	1	d	3	9	1	0	3	0	0	0	0	0	0
4	a	a	a	a	a	a	a	a	d	3	9	1	d	3	9	1	0	4	0	0	0	0	0	0
5	a	a	a	a	a	a	a	a	d	3	9	1	d	3	9	1	9	5	0	0	0	0	F	F
6	a	a	a	a	a	a	a	a	d	3	9	1	d	3	9	1	0	0	0	0	0	0	0	0
7	a	a	a	a	a	a	a	a	d	3	9	1	d	3	9	1	0	1	0	0	0	0	0	0
8	a	a	a	a	a	a	a	a	d	3	9	1	d	3	9	1	0	2	0	0	0	0	0	0
9	a	a	a	a	a	a	a	a	d	3	9	1	d	3	9	1	0	3	0	0	0	0	0	0
10	a	a	a	a	a	a	a	a	d	3	9	1	d	3	9	1	0	4	0	0	0	0	0	0
11	a	a	a	a	a	a	a	a	d	3	9	1	d	3	9	1	9	5	0	0	0	0	F	F
12	a	a	a	a	a	a	a	a	d	3	9	1	d	3	9	1	0	0	0	0	0	0	0	0

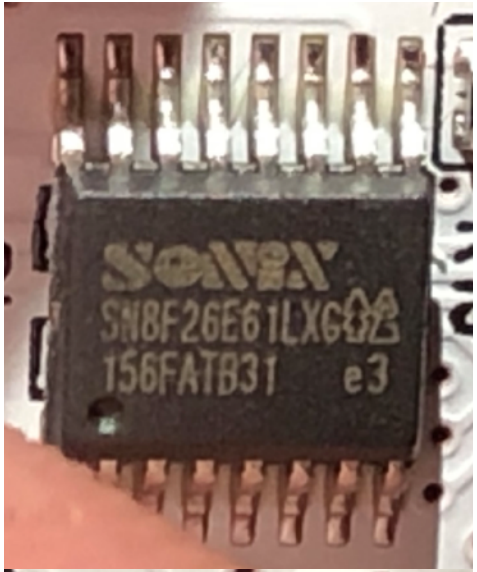


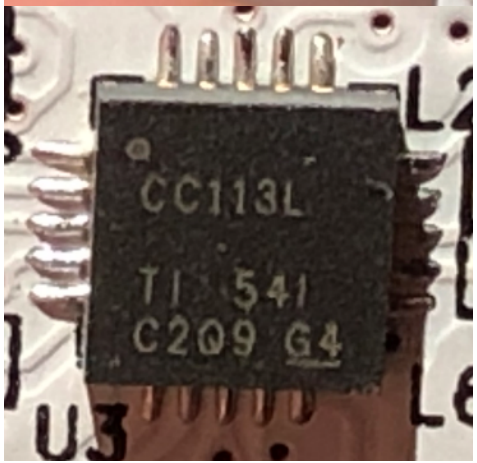
#0000FF

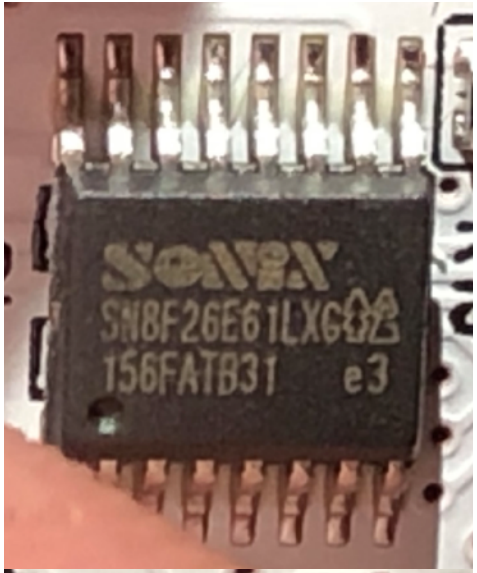
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
1	a	a	a	a	a	a	a	a	d	3	9	1	d	3	9	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0
2	a	a	a	a	a	a	a	a	d	3	9	1	d	3	9	1	0	2	0	0	0	0	0	0	0	0	0	0	0	0
3	a	a	a	a	a	a	a	a	d	3	9	1	d	3	9	1	0	3	0	0	0	0	0	0	0	0	0	0	0	0
4	a	a	a	a	a	a	a	a	d	3	9	1	d	3	9	1	0	4	0	0	0	0	0	0	0	0	0	0	0	0
5	a	a	a	a	a	a	a	a	d	3	9	1	d	3	9	1	9	5	0	0	0	0	F	F	0	0	0	0	0	0
6	a	a	a	a	a	a	a	a	d	3	9	1	d	3	9	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	a	a	a	a	a	a	a	a	d	3	9	1	d	3	9	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0
8	a	a	a	a	a	a	a	a	d	3	9	1	d	3	9	1	0	2	0	0	0	0	0	0	0	0	0	0	0	0
9	a	a	a	a	a	a	a	a	d	3	9	1	d	3	9	1	0	3	0	0	0	0	0	0	0	0	0	0	0	0
10	a	a	a	a	a	a	a	a	d	3	9	1	d	3	9	1	0	4	0	0	0	0	0	0	0	0	0	0	0	0
11	a	a	a	a	a	a	a	a	d	3	9	1	d	3	9	1	9	5	0	0	0	0	F	F	0	0	0	0	0	0
12	a	a	a	a	a	a	a	a	d	3	9	1	d	3	9	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0

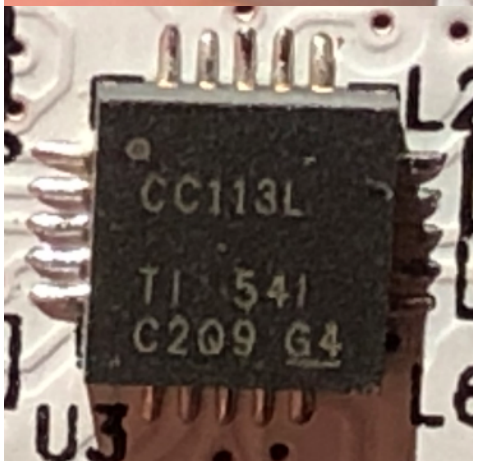
RGB1 RGB2

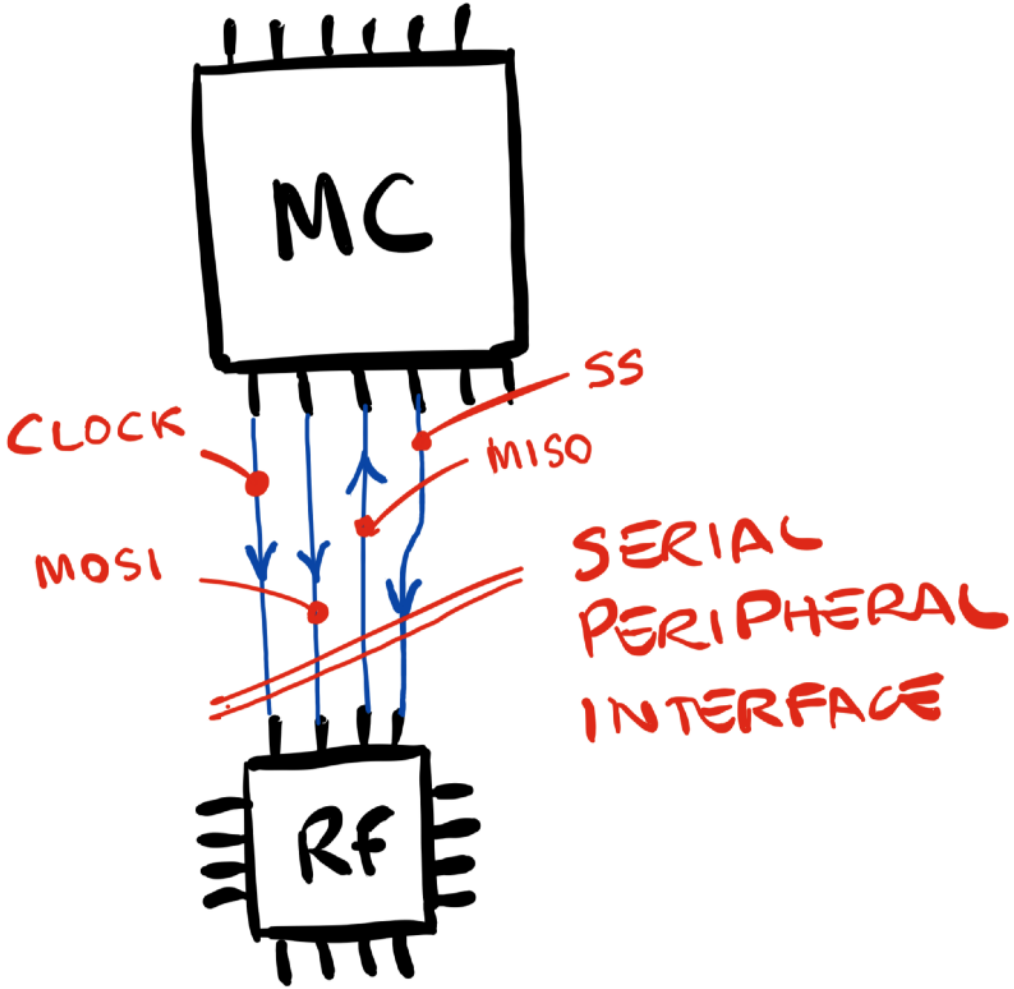
Done!


SONY
SN8F26E61LXG
156FATB31 e3

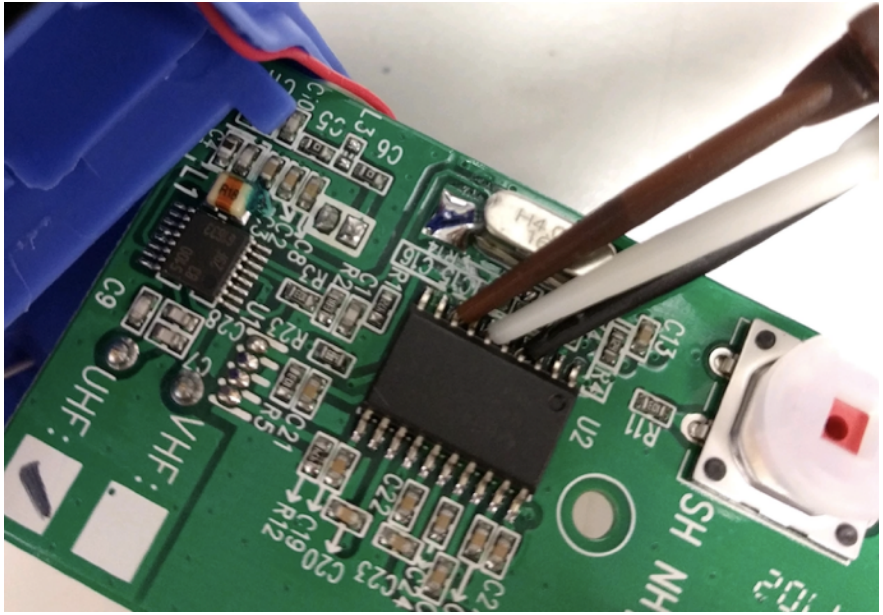

CC113L
TI 541
C209 G4
U3

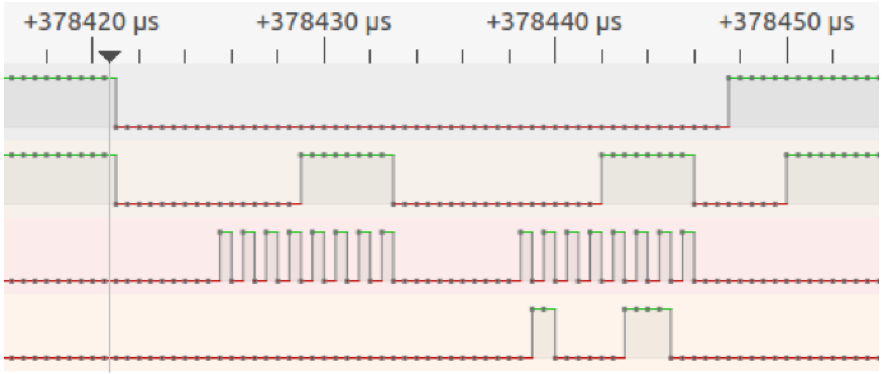

SONY
SN8F26E61LXG
156FATB31 e3

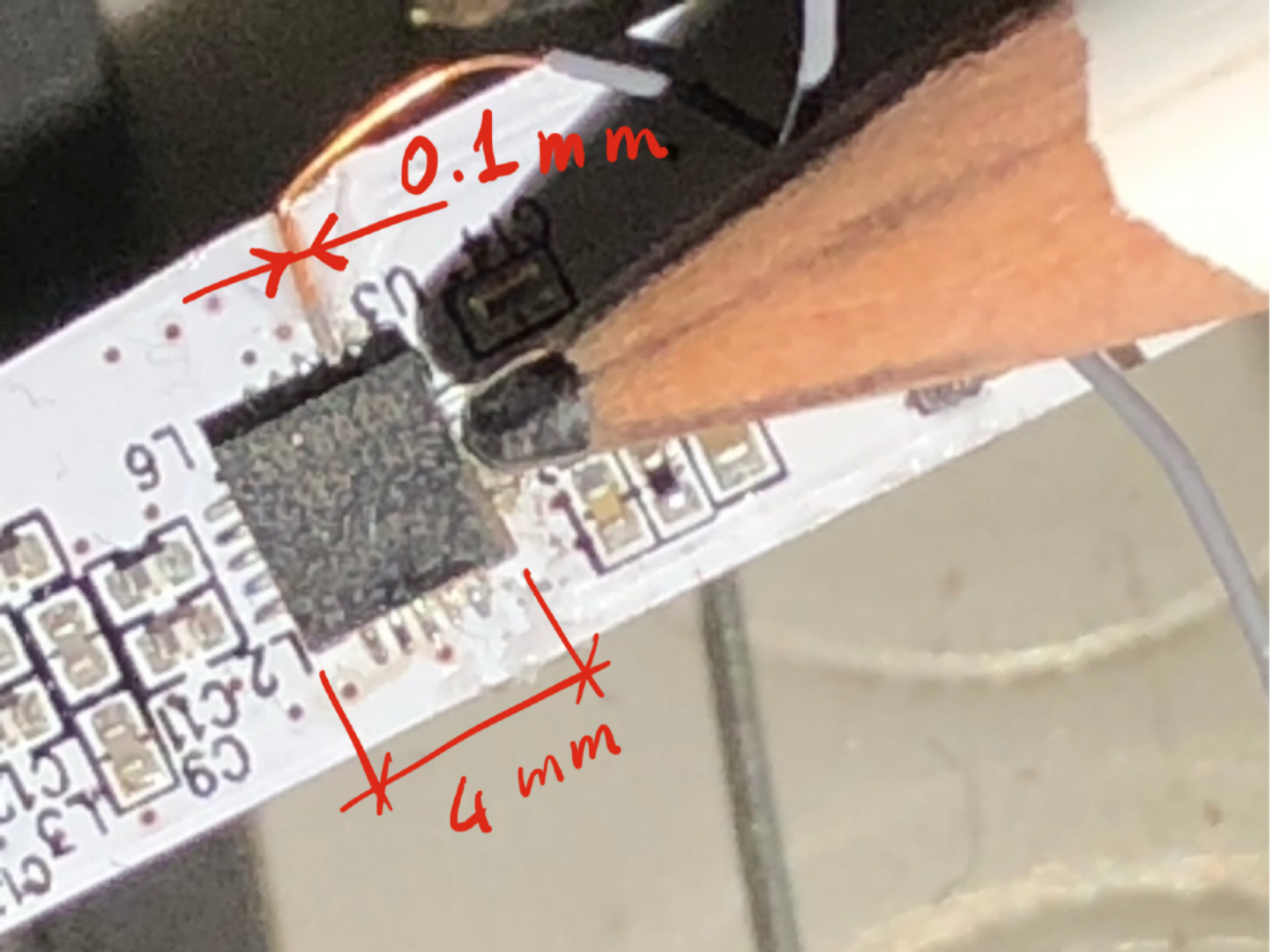

CC113L
TI 541
C209 G4
U3

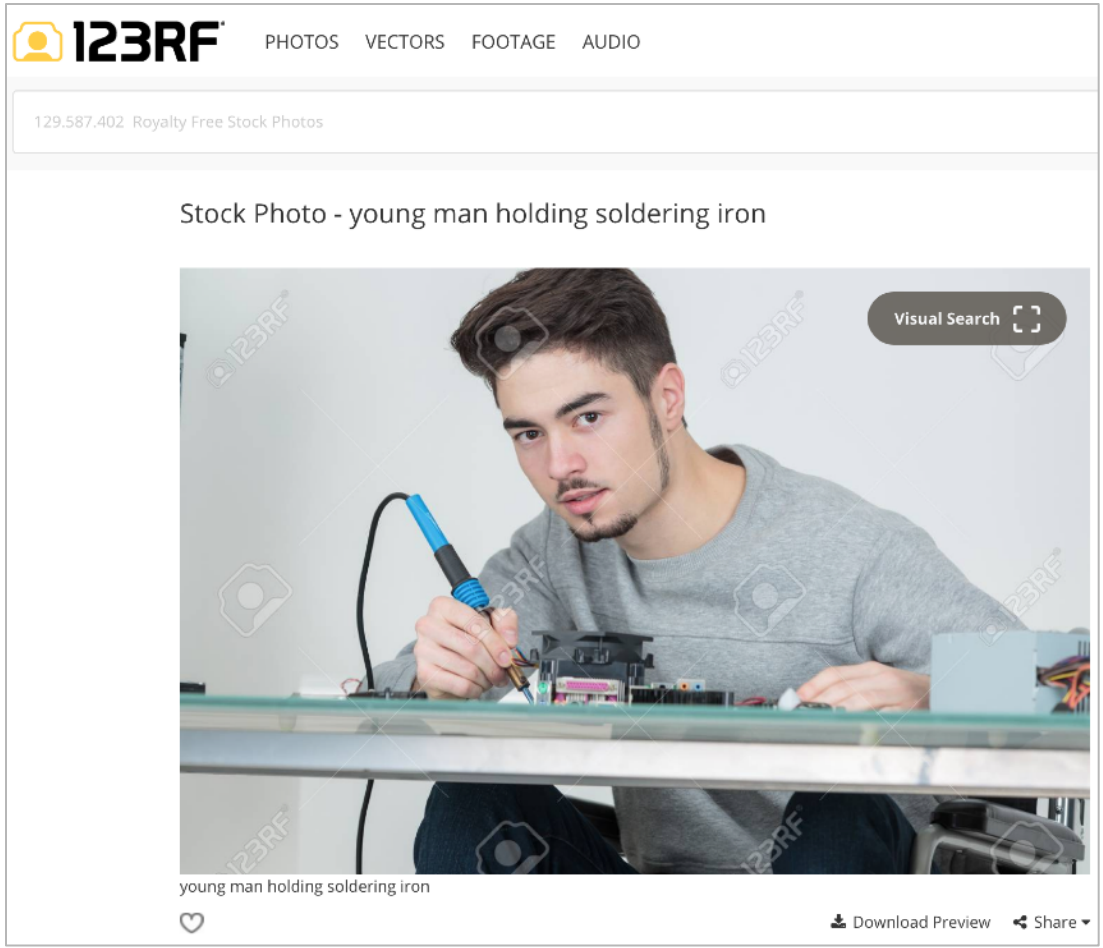

MC
CLOCK
SS
MISO
MOSI
SERIAL
PERIPHERAL
INTERFACE
RF


saleae

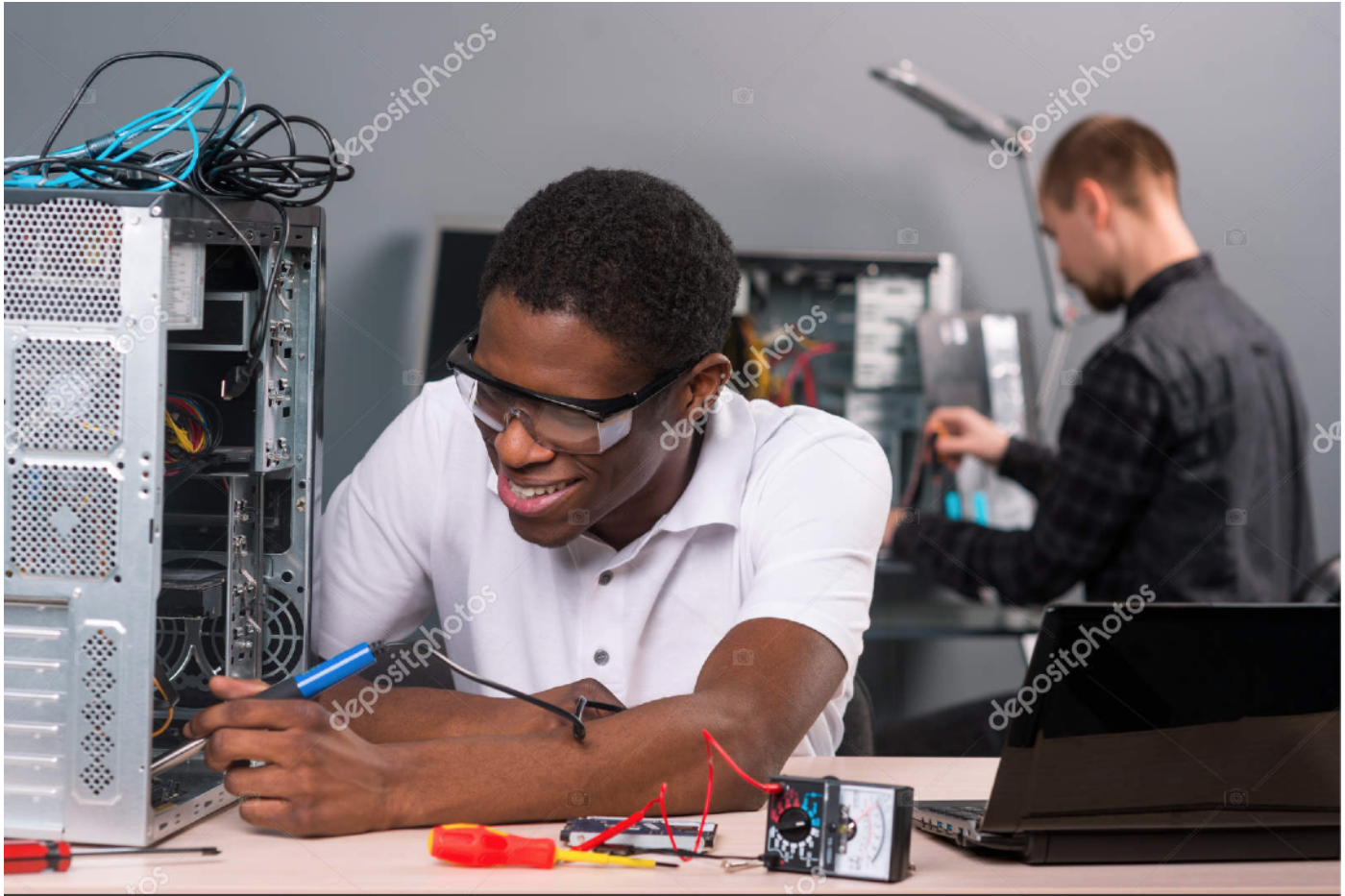


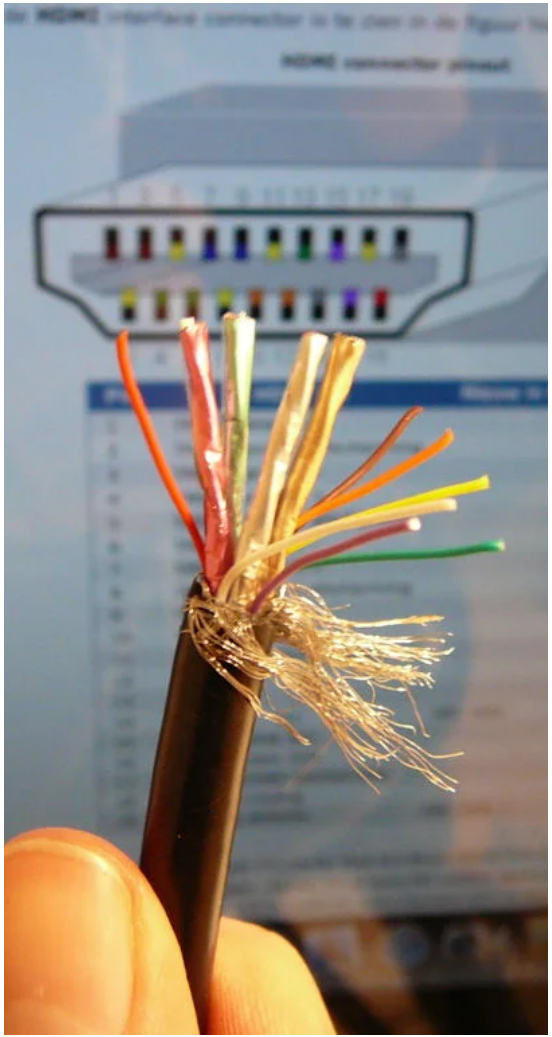

+378420 µs
+378430 µs
+378440 µs
+378450 µs

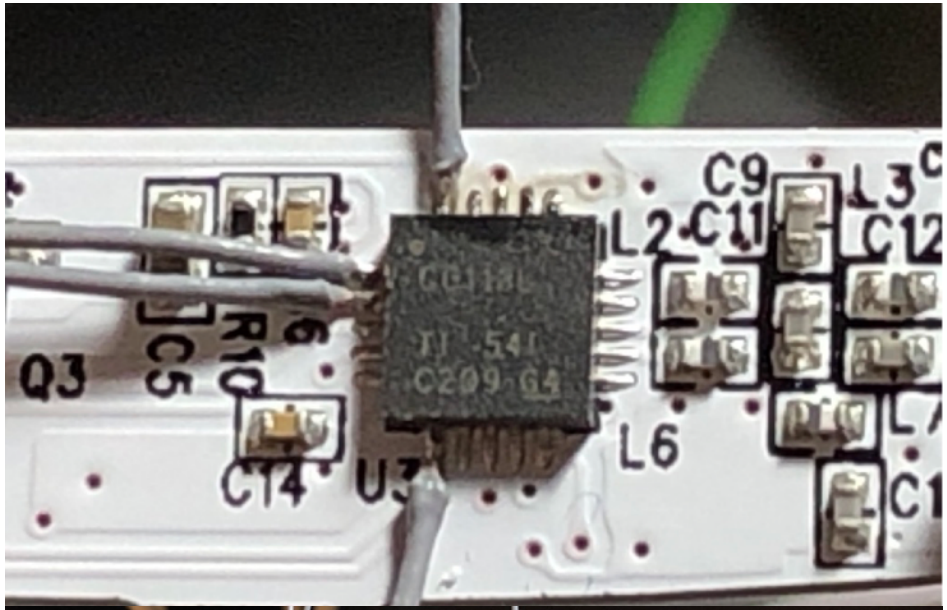

0.1 mm
4 mm

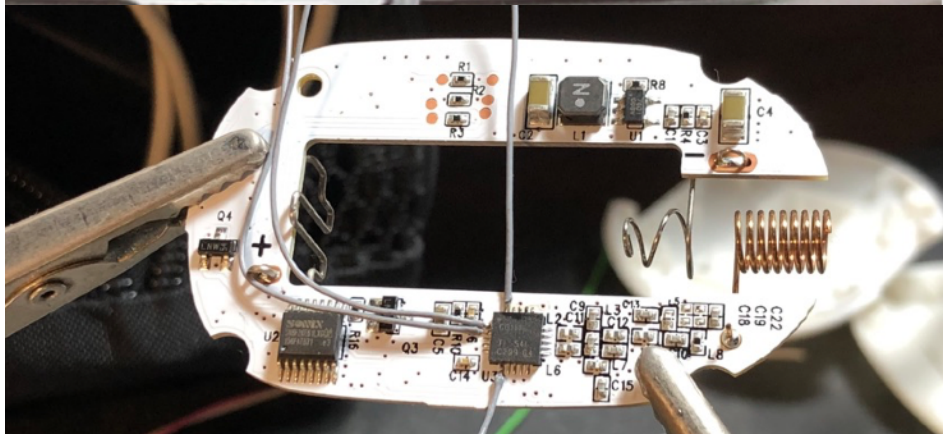


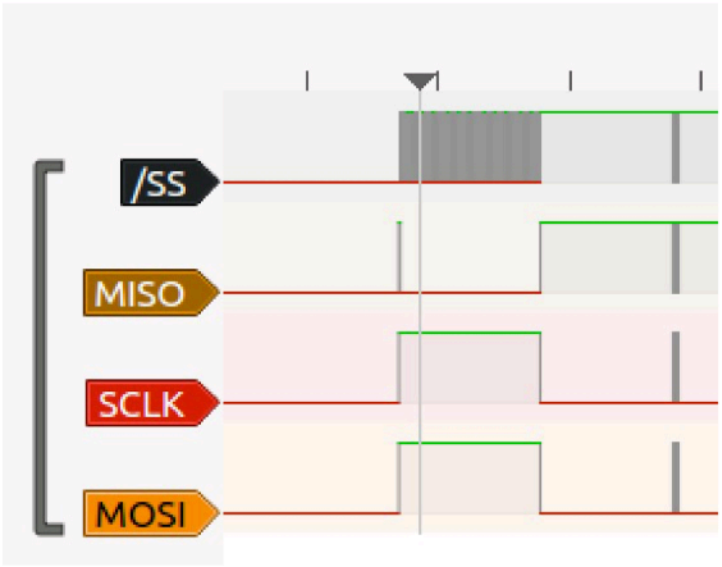
Soldering is no joke! https://www.123rf.com/photo_99185814_young-man-holding-soldering-iron.html

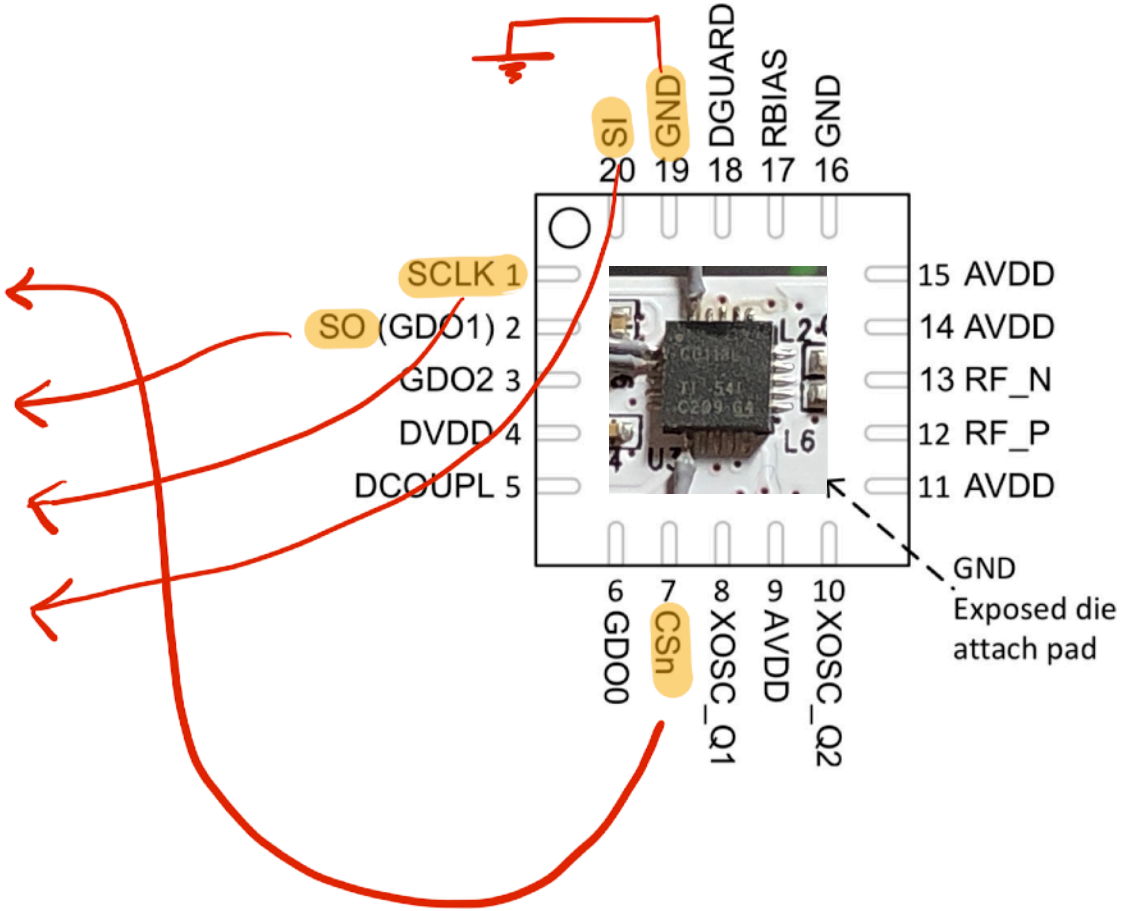

depositphotos
Image ID: 151222084
www.depositphotos.com



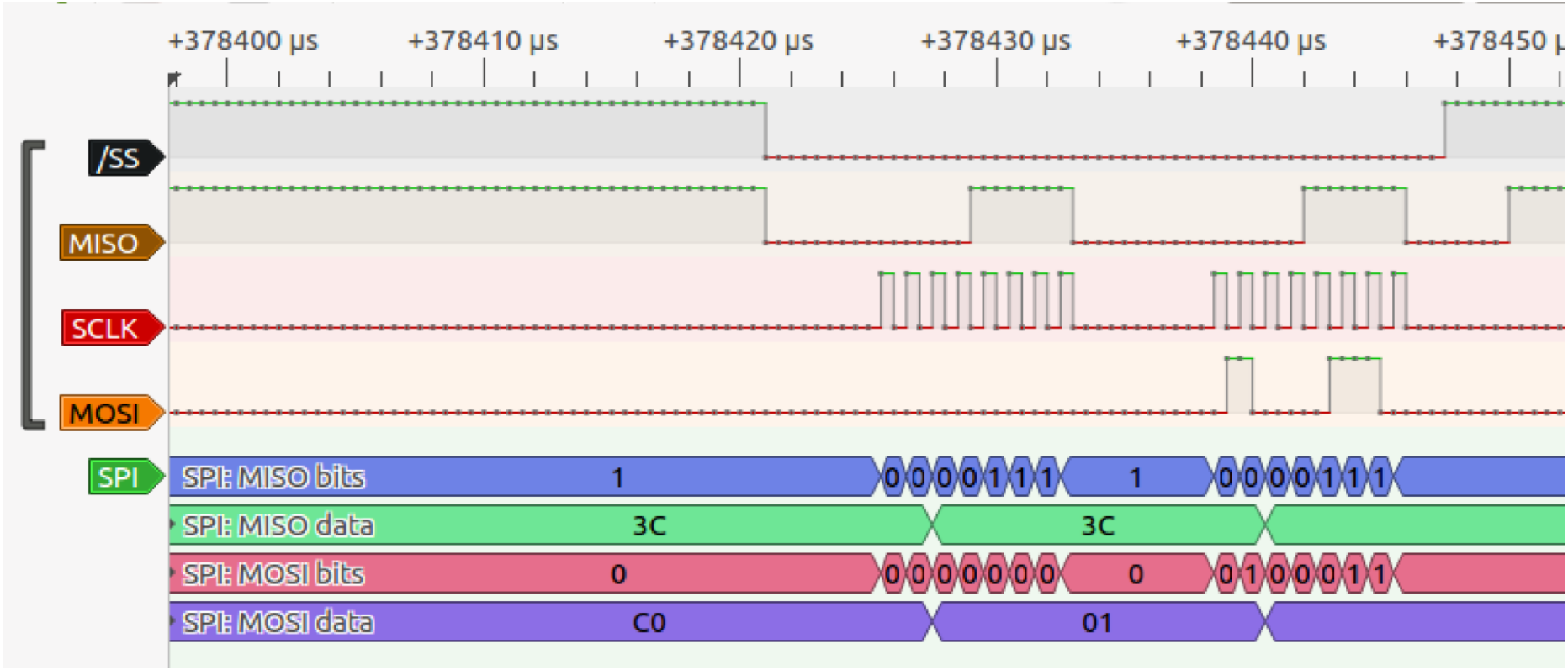

C9
L3
C11
C12
L2
Q3
C5
R6
C14
U3
L6

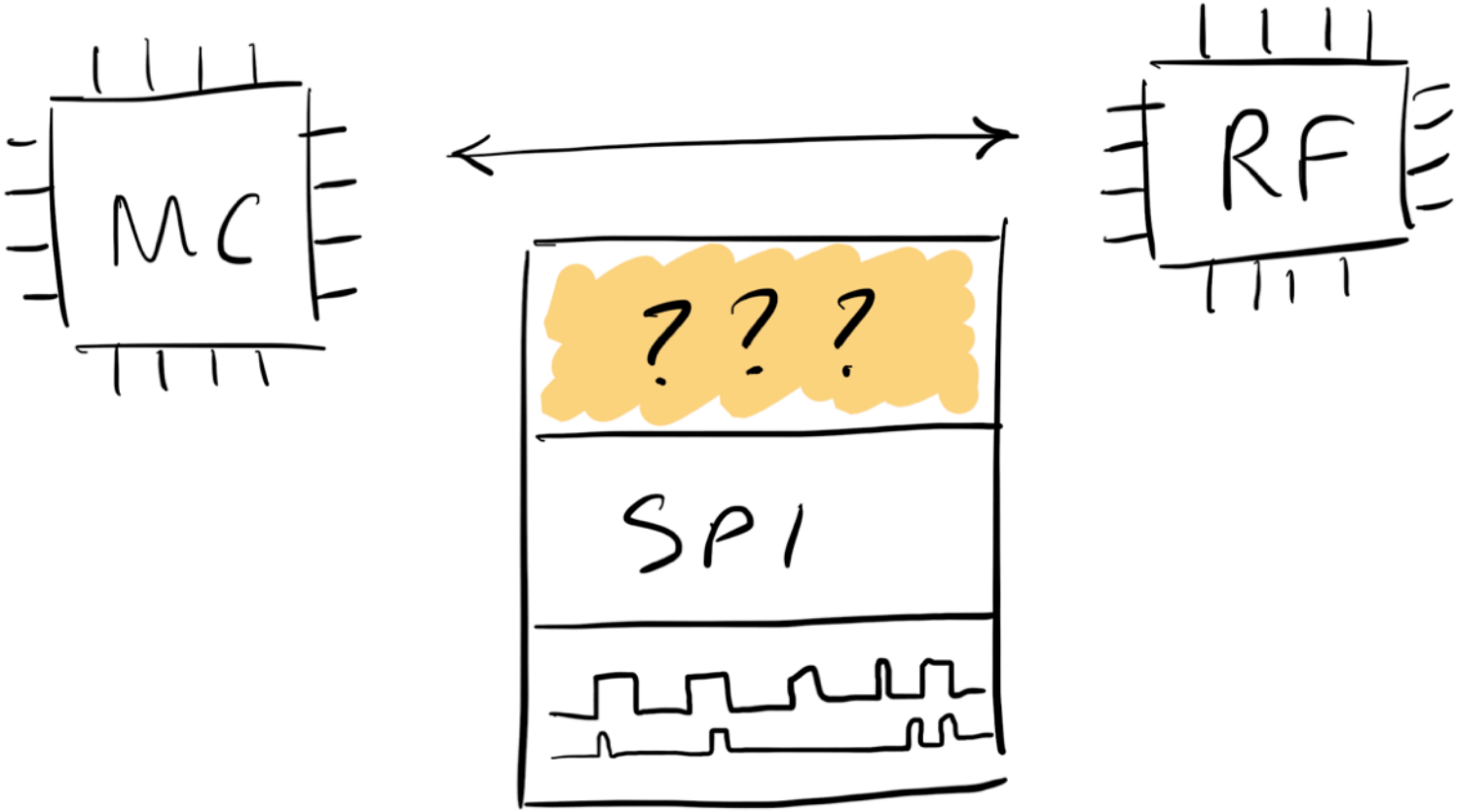


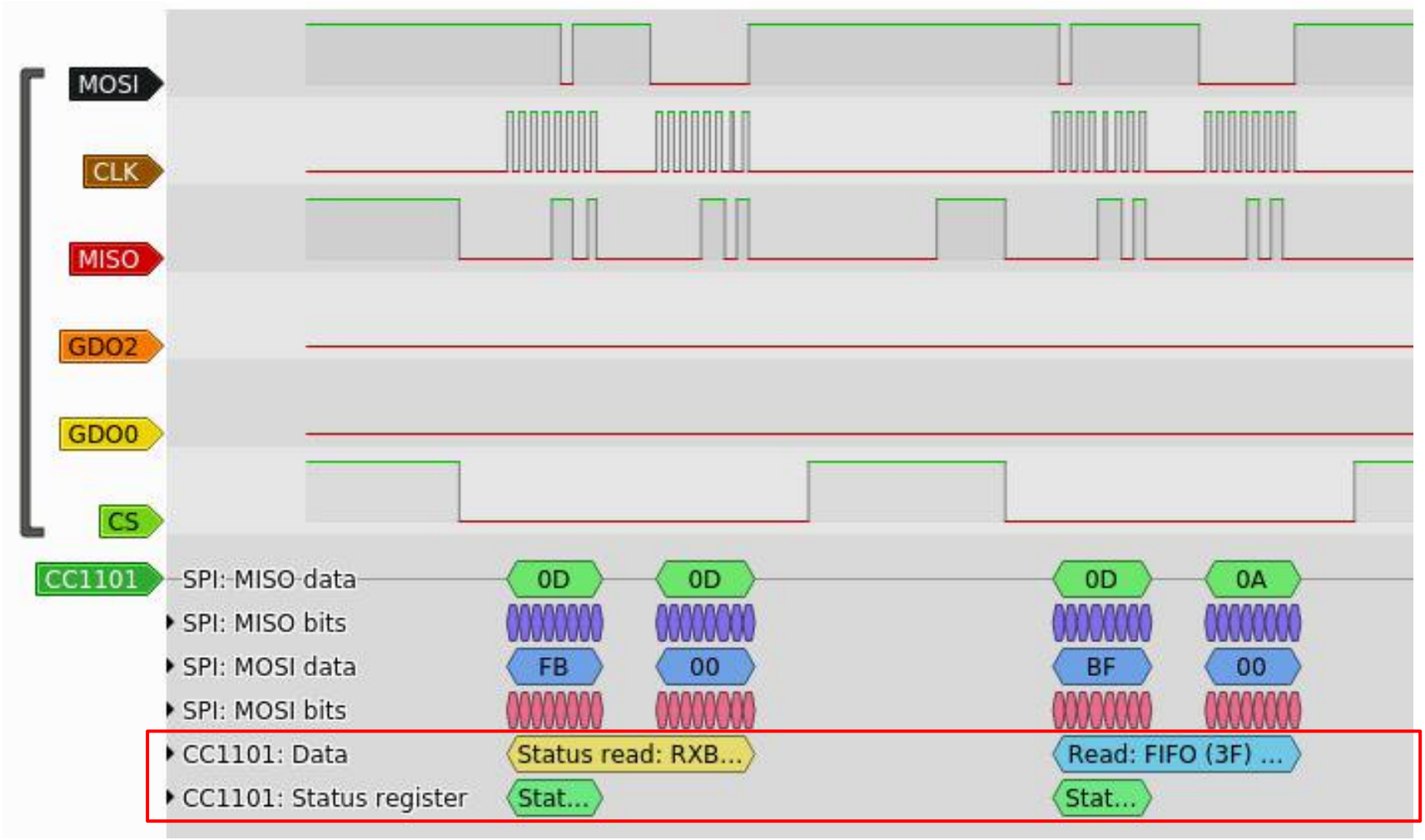




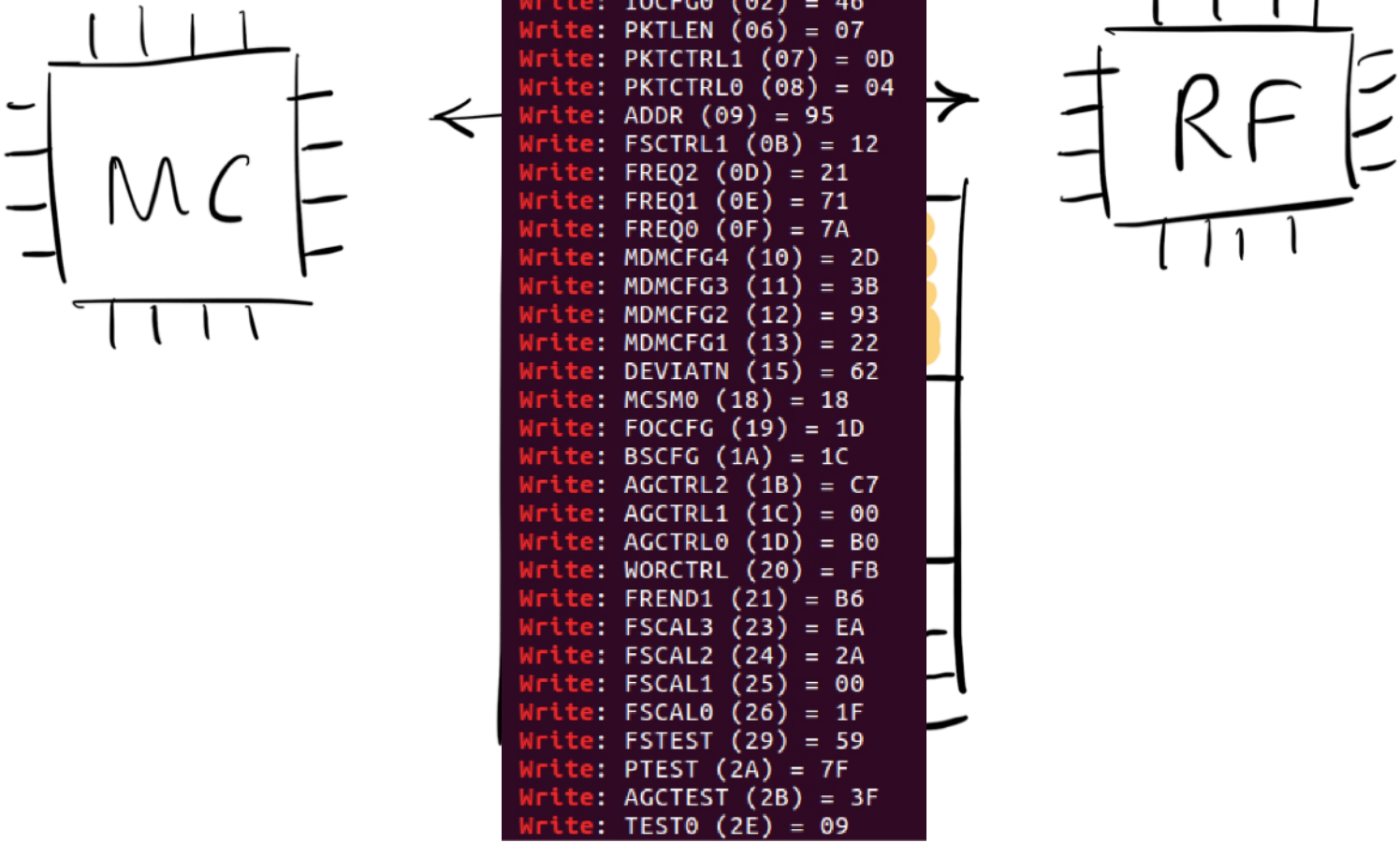
sigrok


+378400 µs
+378410 µs
+378420 µs
+378430 µs
+378440 µs
+378450 µ
/SS
MISO
SCLK
MOSI
SPI
SPI: MISO bits
1
0 0 0 0 1 1 1
1
0 0 0 0 1 1 1
SPI: MISO data
3C
3C
SPI: MOSI bits
0
0 0 0 0 0 0 0
0
0 1 0 0 0 1 1
SPI: MOSI data
C0
01


MC
???
SPI
RF


MOSI
CLK
MISO
GDO2
GDO0
CS
CC1101
SPI: MISO data
SPI: MISO bits
SPI: MOSI data
SPI: MOSI bits
CC1101: Data
CC1101: Status register
0D
0D
0D
0A
FB
00
BF
00
Status read: RXB...
Read: FIFO (3F) ...
Stat...
Stat...

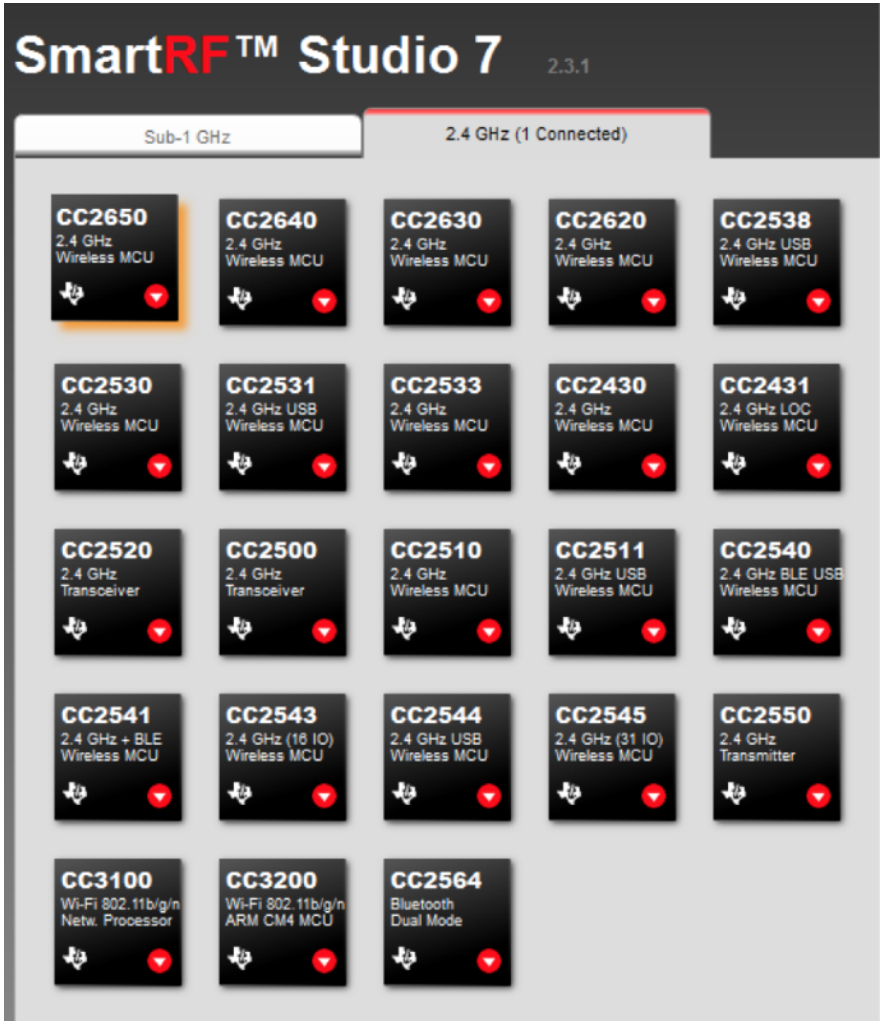
```
$ sigrok-cli --continuous \
    -P spi:clk=SCLK:mosi=MOSI:miso=MISO:cs=SS,cc1101 -A cc1101 \
    --channels D0=SS,D1=MISO,D2=SCLK,D3=MOSI \
    --config "samplerate=2 MHz"
```

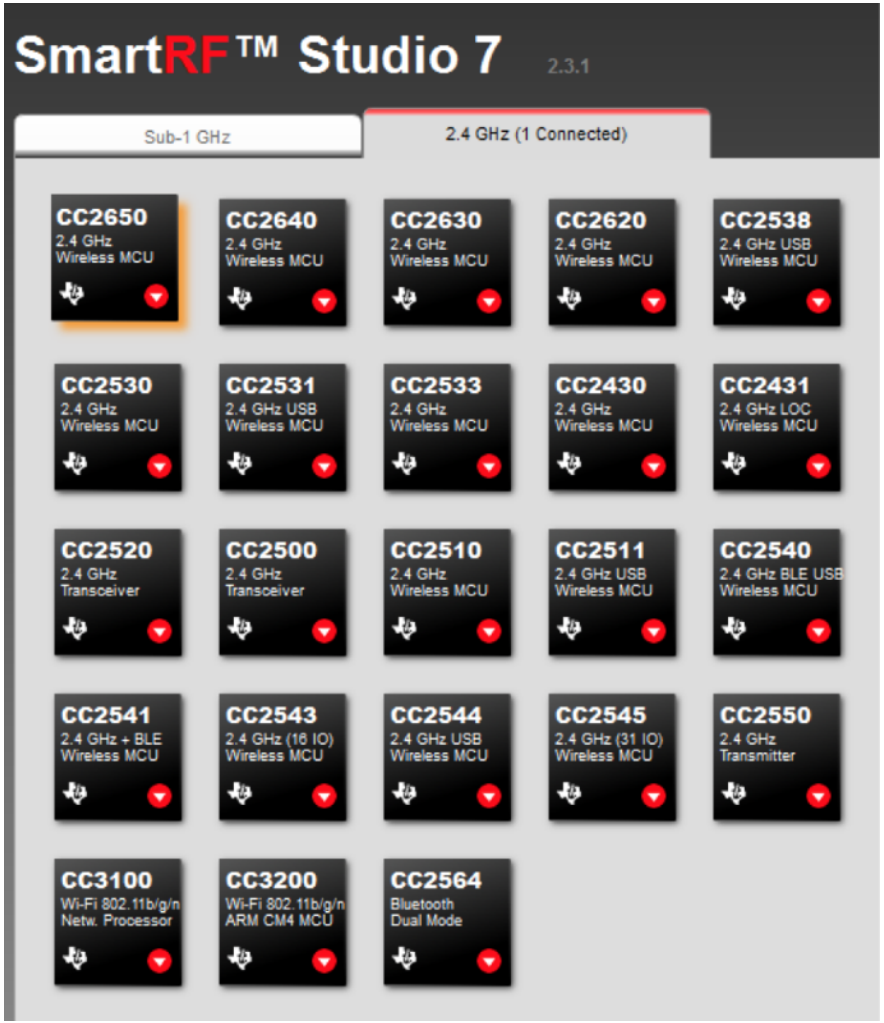

MC
RF
Write: IOCFG2 (00) = 46
Write: IOCFG0 (02) = 46
Write: PKTLEN (06) = 07
Write: PKTCTRL1 (07) = 0D
Write: PKTCTRL0 (08) = 04
Write: ADDR (09) = 95
Write: FSCTRL1 (0B) = 12
Write: FREQ2 (0D) = 21
Write: FREQ1 (0E) = 71
Write: FREQ0 (0F) = 7A
Write: MDMCFG4 (10) = 2D
Write: MDMCFG3 (11) = 3B
Write: MDMCFG2 (12) = 93
Write: MDMCFG1 (13) = 22
Write: DEVIATN (15) = 62
Write: MCSM0 (18) = 18
Write: FOCCFG (19) = 1D
Write: BSCFG (1A) = 1C
Write: AGCTRL2 (1B) = C7
Write: AGCTRL1 (1C) = 00
Write: AGCTRL0 (1D) = B0
Write: WORCTRL (20) = FB
Write: FREND1 (21) = B6
Write: FSCAL3 (23) = EA
Write: FSCAL2 (24) = 2A
Write: FSCAL1 (25) = 00
Write: FSCAL0 (26) = 1F
Write: FSTEST (29) = 59
Write: PTEST (2A) = 7F
Write: AGCTEST (2B) = 3F
Write: TEST0 (2E) = 09

```
Write: IOCFG2 (00) = 46
Write: IOCFG0 (02) = 46
Write: PKTLEN (06) = 07
Write: PKTCTRL1 (07) = 0D
Write: PKTCTRL0 (08) = 04
Write: ADDR (09) = 95
Write: FSCTRL1 (0B) = 12
Write: FREQ2 (0D) = 21
Write: FREQ1 (0E) = 71
Write: FREQ0 (0F) = 7A
Write: MDMCFG4 (10) = 2D
Write: MDMCFG3 (11) = 3B
Write: MDMCFG2 (12) = 93
Write: MDMCFG1 (13) = 22
Write: DEVIATN (15) = 62
Write: MCSM0 (18) = 18
Write: FOCCFG (19) = 1D
Write: BSCFG (1A) = 1C
Write: AGCTRL2 (1B) = C7
Write: AGCTRL1 (1C) = 00
Write: AGCTRL0 (1D) = B0
Write: WORCTRL (20) = FB
Write: FREND1 (21) = B6
Write: FSCAL3 (23) = EA
Write: FSCAL2 (24) = 2A
Write: FSCAL1 (25) = 00
Write: FSCAL0 (26) = 1F
Write: FSTEST (29) = 59
Write: PTEST (2A) = 7F
Write: AGCTEST (2B) = 3F
Write: TEST0 (2E) = 09
```

Table 5-31. 0x0B: FSCTRL1 - Frequency Synthesizer Control

Bit	Field Name	Reset	R/W	Description
7:6			R0	Not used
5		0	R/W	Use setting from SmartRF Studio
4:0	FREQ_IF[4:0]	15 (01111)	R/W	The desired IF frequency to employ in RX. Subtracted from FS base frequency in RX and controls the digital complex mixer in the demodulator. $f_{IF} = \frac{f_{XOSC}}{2^{10}} \cdot FREQ\_IF$ The default value gives an IF frequency of 381kHz, assuming a 26.0 MHz crystal.


SmartRF™ Studio 7
2.3.1
Sub-1 GHz
2.4 GHz (1 Connected)
CC2650
2.4 GHz
Wireless MCU
CC2640
2.4 GHz
Wireless MCU
CC2630
2.4 GHz
Wireless MCU
CC2620
2.4 GHz
Wireless MCU
CC2538
2.4 GHz USB
Wireless MCU
CC2530
2.4 GHz
Wireless MCU
CC2531
2.4 GHz USB
Wireless MCU
CC2533
2.4 GHz
Wireless MCU
CC2430
2.4 GHz
Wireless MCU
CC2431
2.4 GHz LOC
Wireless MCU
CC2520
2.4 GHz
Transceiver
CC2500
2.4 GHz
Transceiver
CC2510
2.4 GHz
Wireless MCU
CC2511
2.4 GHz USB
Wireless MCU
CC2540
2.4 GHz BLE USB
Wireless MCU
CC2541
2.4 GHz + BLE
Wireless MCU
CC2543
2.4 GHz (16 IO)
Wireless MCU
CC2544
2.4 GHz USB
Wireless MCU
CC2545
2.4 GHz (31 IO)
Wireless MCU
CC2550
2.4 GHz
Transmitter
CC3100
Wi-Fi 802.11b/g/n
Netw. Processor
CC3200
Wi-Fi 802.11b/g/n
ARM CM4 MCU
CC2564
Bluetooth
Dual Mode

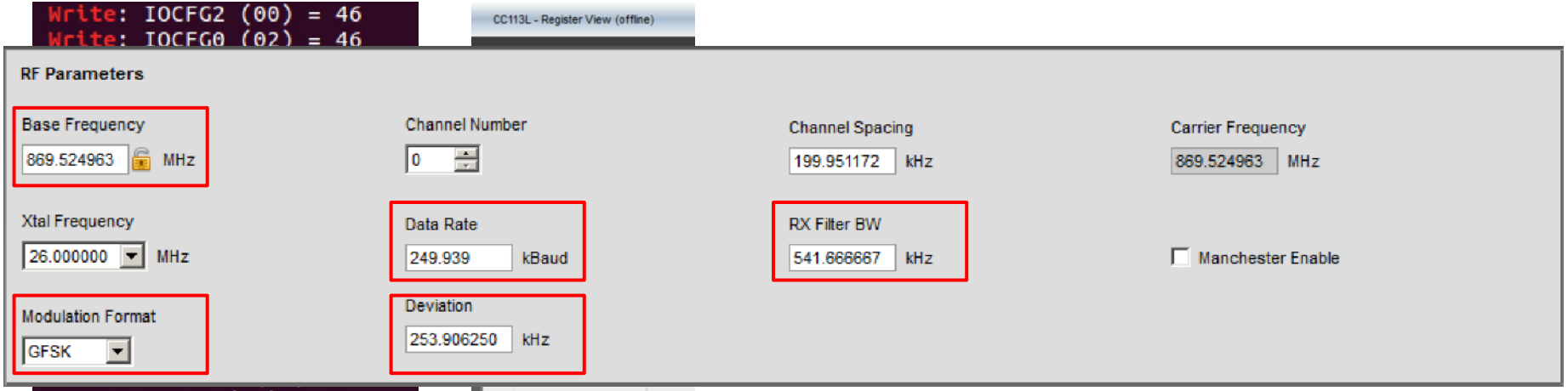



```
Write: IOCFG2 (00) = 46
Write: IOCFG0 (02) = 46
Write: PKTLEN (06) = 07
Write: PKTCTRL1 (07) = 0D
Write: PKTCTRL0 (08) = 04
Write: ADDR (09) = 95
Write: FSCTRL1 (0B) = 12
Write: FREQ2 (0D) = 21
Write: FREQ1 (0E) = 71
Write: FREQ0 (0F) = 7A
Write: MDMCFG4 (10) = 2D
Write: MDMCFG3 (11) = 3B
Write: MDMCFG2 (12) = 93
Write: MDMCFG1 (13) = 22
Write: DEVIATN (15) = 62
Write: MCSM0 (18) = 18
Write: FOCCFG (19) = 1D
Write: BSCFG (1A) = 1C
Write: AGCTRL2 (1B) = C7
Write: AGCTRL1 (1C) = 00
Write: AGCTRL0 (1D) = B0
Write: WORCTRL (20) = FB
Write: FREND1 (21) = B6
Write: FSCAL3 (23) = EA
Write: FSCAL2 (24) = 2A
Write: FSCAL1 (25) = 00
Write: FSCAL0 (26) = 1F
Write: FSTEST (29) = 59
Write: PTEST (2A) = 7F
Write: AGCTEST (2B) = 3F
Write: TEST0 (2E) = 09
```

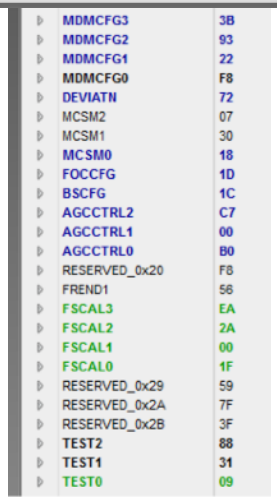
CC113L - Register View (offline)

Register	Value
IOCFG2	46
IOCFG1	46
IOCFG0	07
FIFOTHR	07
SYNC1	D3
SYNC0	91
PKTLEN	07
PKTCTRL1	0D
PKTCTRL0	04
ADDR	95
CHANNR	00
FSCTRL1	0F
FSCTRL0	00
FREQ2	21
FREQ1	71
FREQ0	7A
MDMCFG4	2D
MDMCFG3	3B
MDMCFG2	93
MDMCFG1	22
MDMCFG0	F8
DEVIATN	72
MCSM2	07
MCSM1	30
MCSM0	18
FOCCFG	1D
BSCFG	1C
AGCCTRL2	C7
AGCCTRL1	00
AGCCTRL0	B0
RESERVED_0x20	F8
FREND1	56
FSCAL3	EA
FSCAL2	2A
FSCAL1	00
FSCAL0	1F
RESERVED_0x29	59
RESERVED_0x2A	7F
RESERVED_0x2B	3F
TEST2	88
TEST1	31
TEST0	09

```
Write: IOCFG2 (00) = 46
Write: IOCFG0 (02) = 46
```

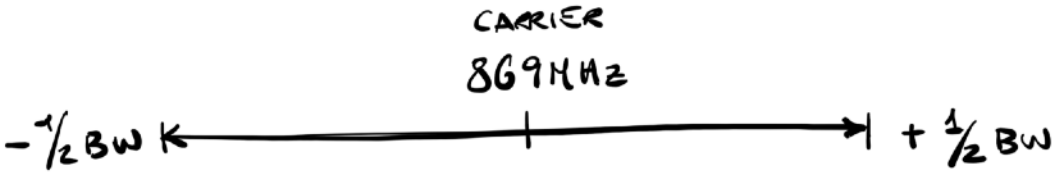


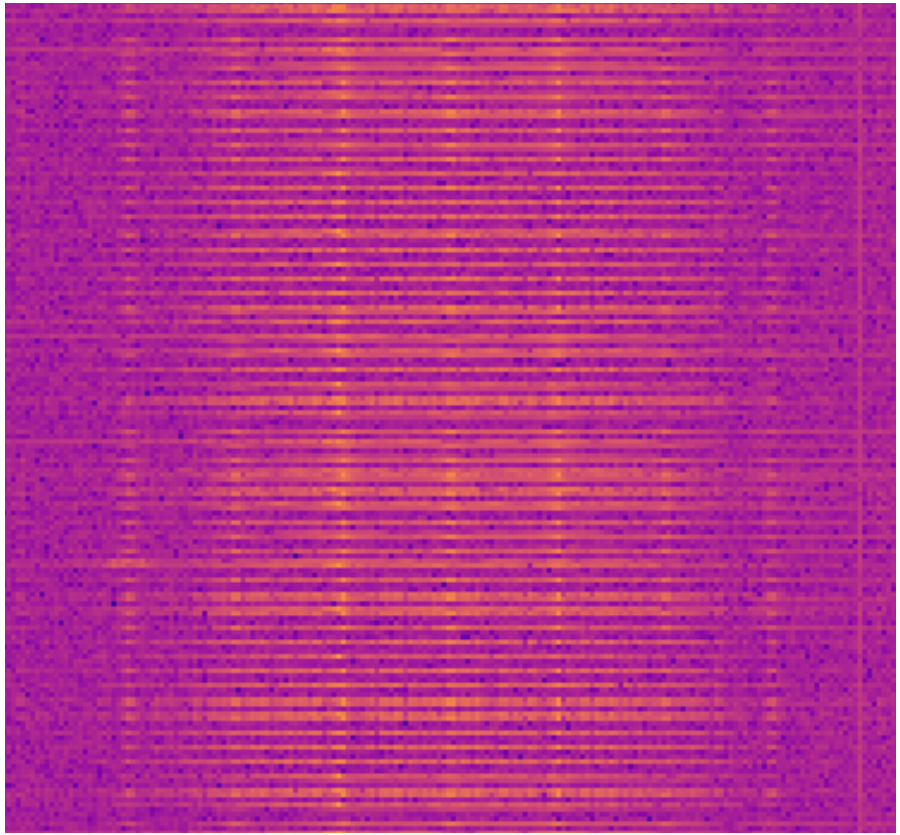

```
Write: MCSM0 (18) = 18
Write: FOCCFG (19) = 1D
Write: BSCFG (1A) = 1C
Write: AGCTRL2 (1B) = C7
Write: AGCTRL1 (1C) = 00
Write: AGCTRL0 (1D) = B0
Write: WORCTRL (20) = FB
Write: FREND1 (21) = B6
Write: FSCAL3 (23) = EA
Write: FSCAL2 (24) = 2A
Write: FSCAL1 (25) = 00
Write: FSCAL0 (26) = 1F
Write: FSTEST (29) = 59
Write: PTEST (2A) = 7F
Write: AGCTEST (2B) = 3F
Write: TEST0 (2E) = 09
```



EXACT PARAMETERS:

- Frequency: 869.524963 MHz
- Data rate: 249.939 kBaud
- Bandwidth: 541.666667 kHz
- Modulation format: GFSK
- Deviation: 253.906250 kHz

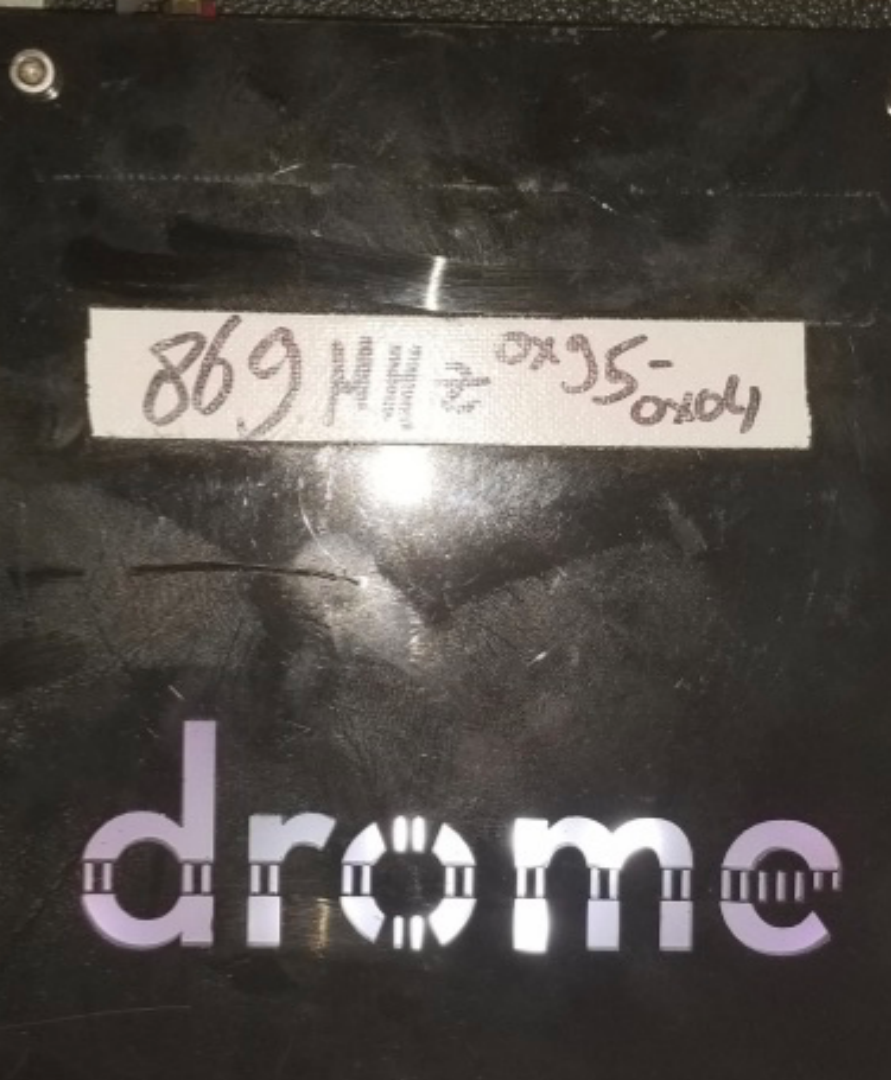


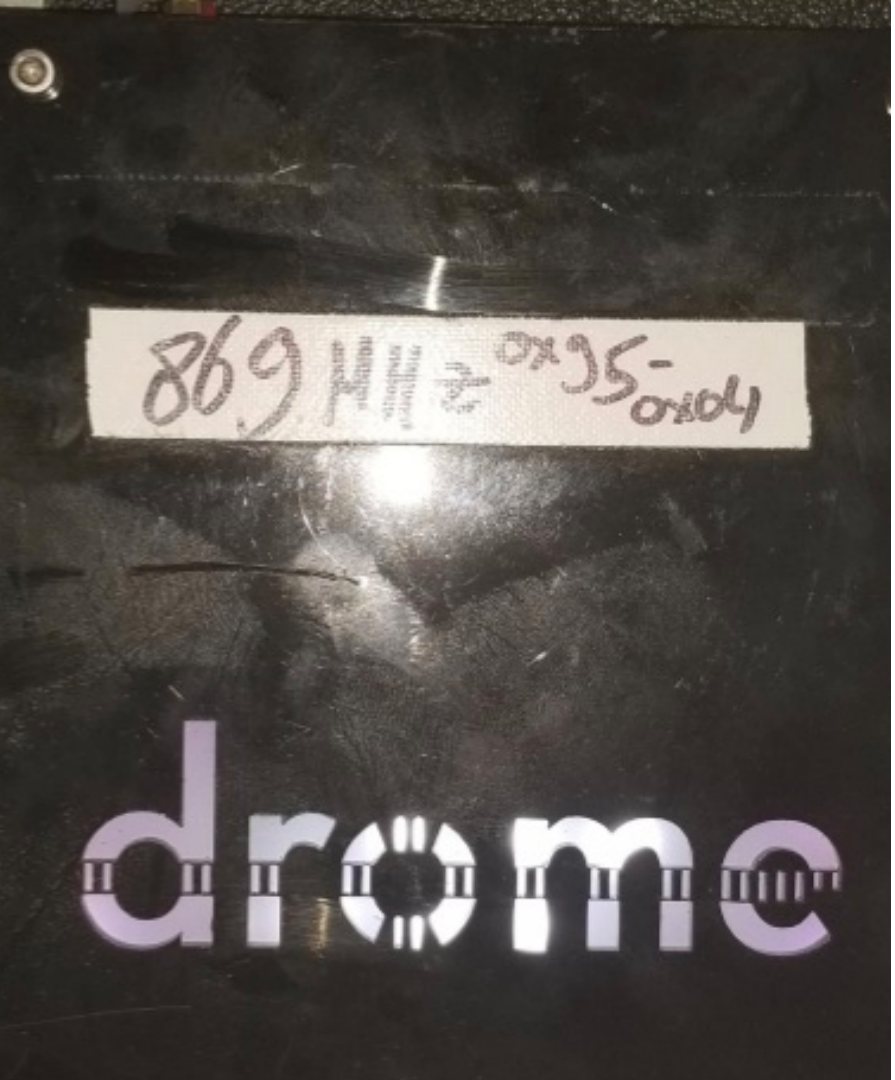


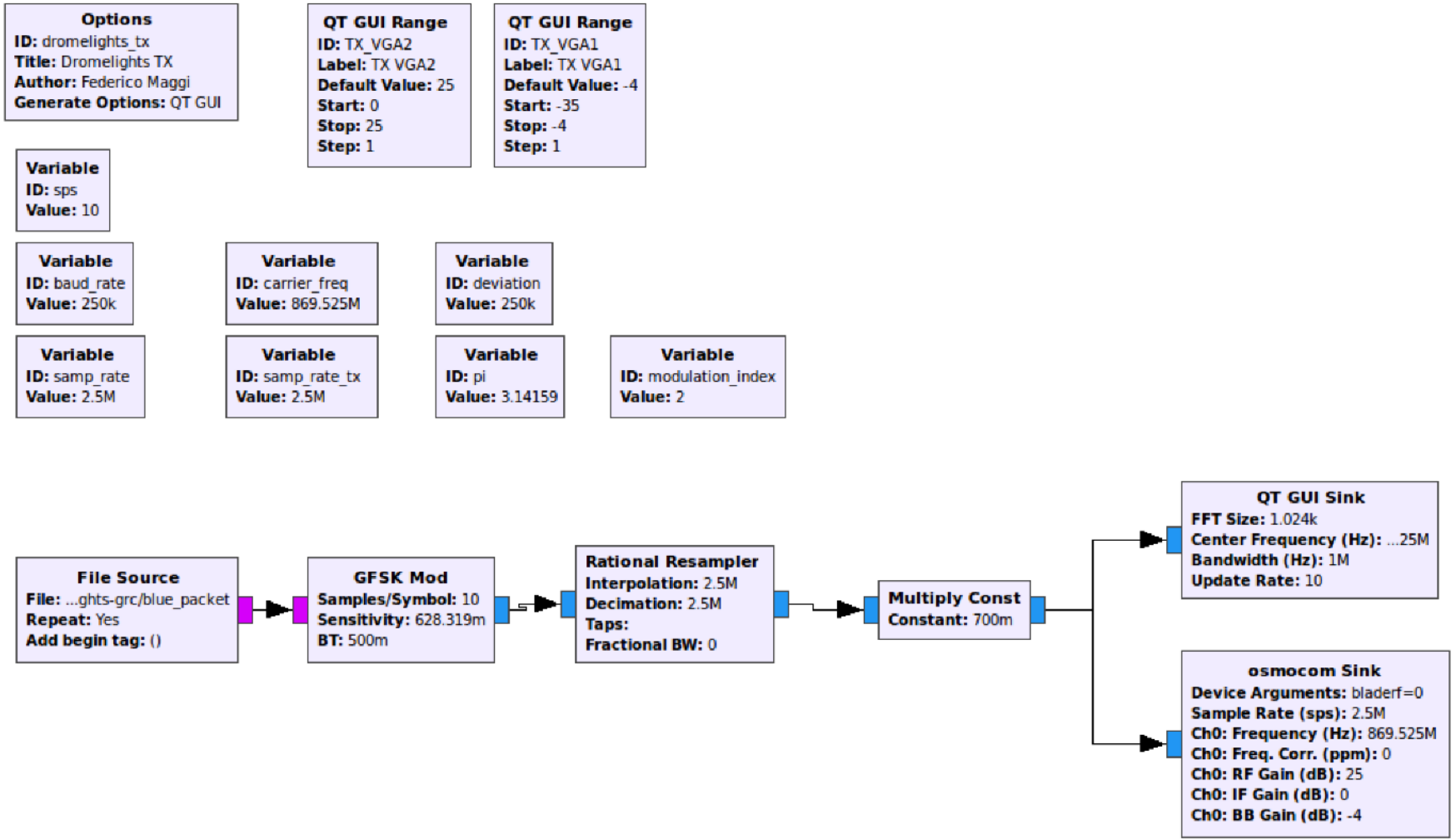
EXACT PARAMETERS:

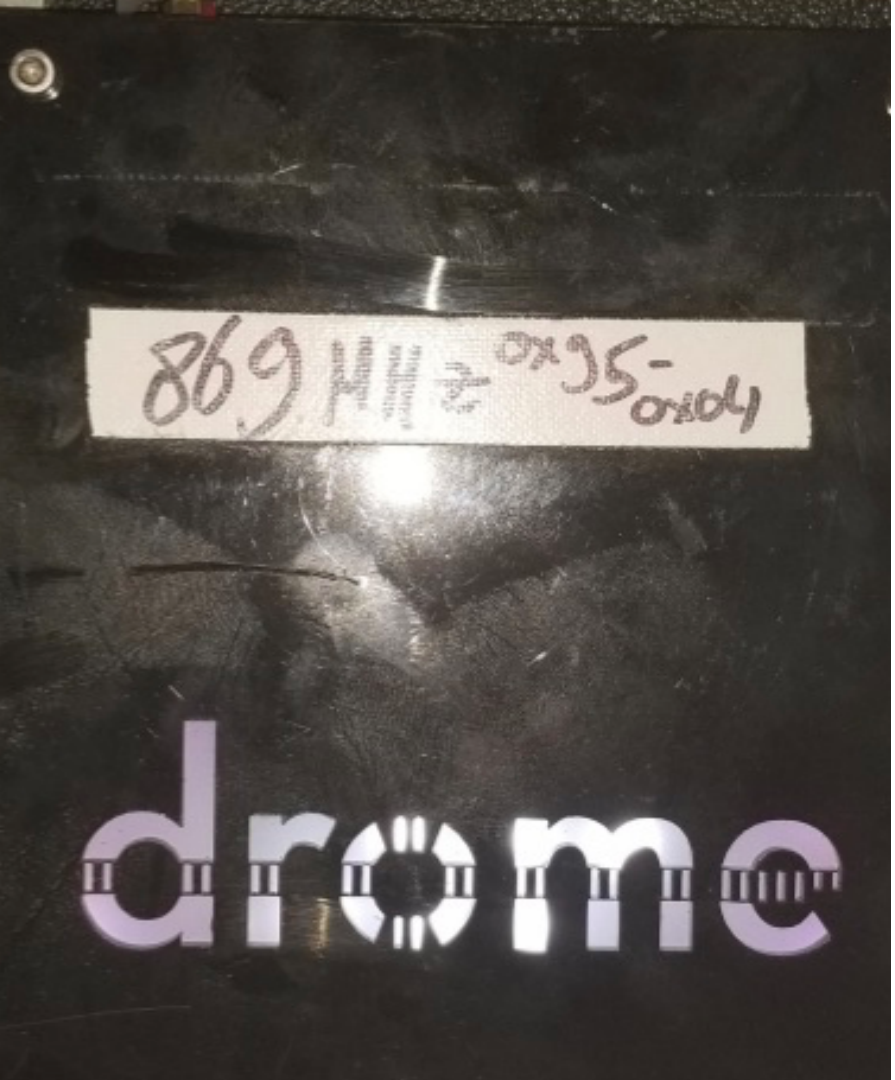
- Frequency: 869.524963 MHz
- Data rate: 249.939 kBaud
- Bandwidth: 541.666667 kHz
- Modulation format: GFSK
- Deviation: 253.906250 kHz

Transmitter design


869 MHz 0x95-0x04
drome

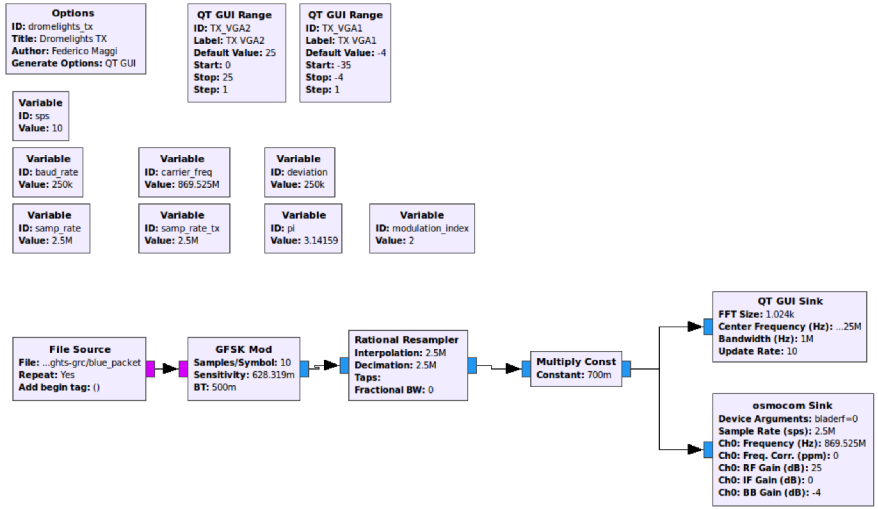

869 MHz 0x95-0x04
drome


Options
ID: dromelights_tx
Title: Dromelights TX
Author: Federico Maggi
Generate Options: QT GUI
QT GUI Range
ID: TX_VGA2
Label: TX VGA2
Default Value: 25
Start: 0
Stop: 25
Step: 1
QT GUI Range
ID: TX_VGA1
Label: TX VGA1
Default Value: -4
Start: -35
Stop: -4
Step: 1
Variable
ID: sps
Value: 10
Variable
ID: baud_rate
Value: 250k
Variable
ID: carrier_freq
Value: 869.525M
Variable
ID: deviation
Value: 250k
Variable
ID: samp_rate
Value: 2.5M
Variable
ID: samp_rate_tx
Value: 2.5M
Variable
ID: pi
Value: 3.14159
Variable
ID: modulation_index
Value: 2
File Source
File: ...ghts-grc/blue_packet
Repeat: Yes
Add begin tag: ()
GFSK Mod
Samples/Symbol: 10
Sensitivity: 628.319m
BT: 500m
Rational Resampler
Interpolation: 2.5M
Decimation: 2.5M
Taps:
Fractional BW: 0
Multiply Const
Constant: 700m
QT GUI Sink
FFT Size: 1.024k
Center Frequency (Hz): ...25M
Bandwidth (Hz): 1M
Update Rate: 10
osmocom Sink
Device Arguments: bladerf=0
Sample Rate (sps): 2.5M
Ch0: Frequency (Hz): 869.525M
Ch0: Freq. Corr. (ppm): 0
Ch0: RF Gain (dB): 25
Ch0: IF Gain (dB): 0
Ch0: BB Gain (dB): -4

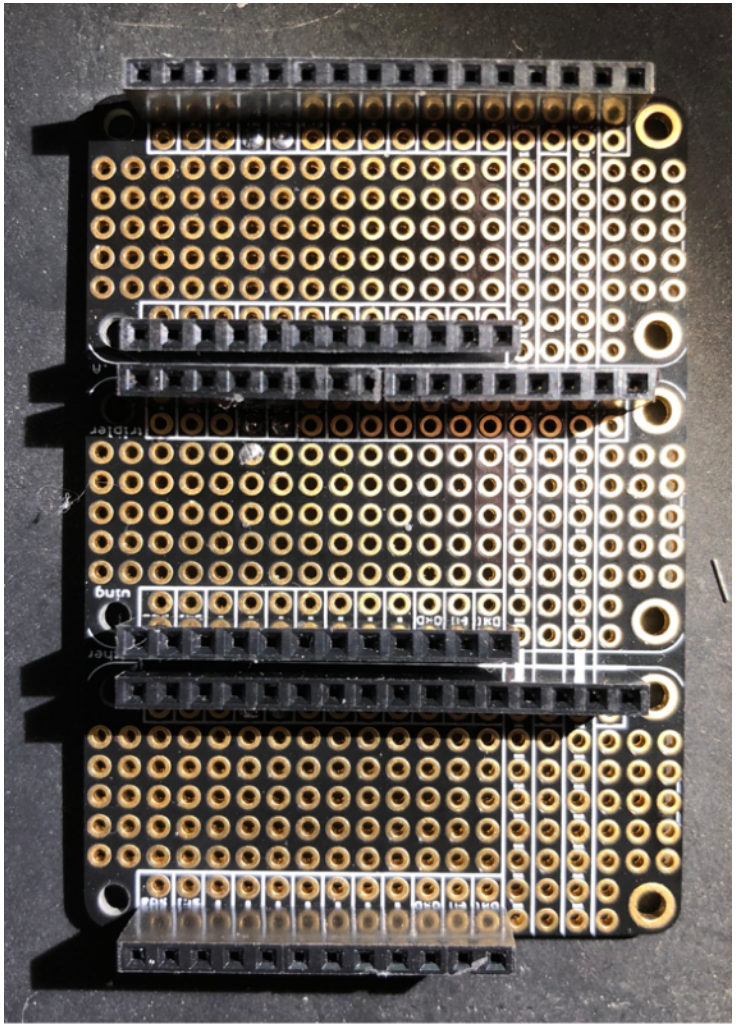

drome

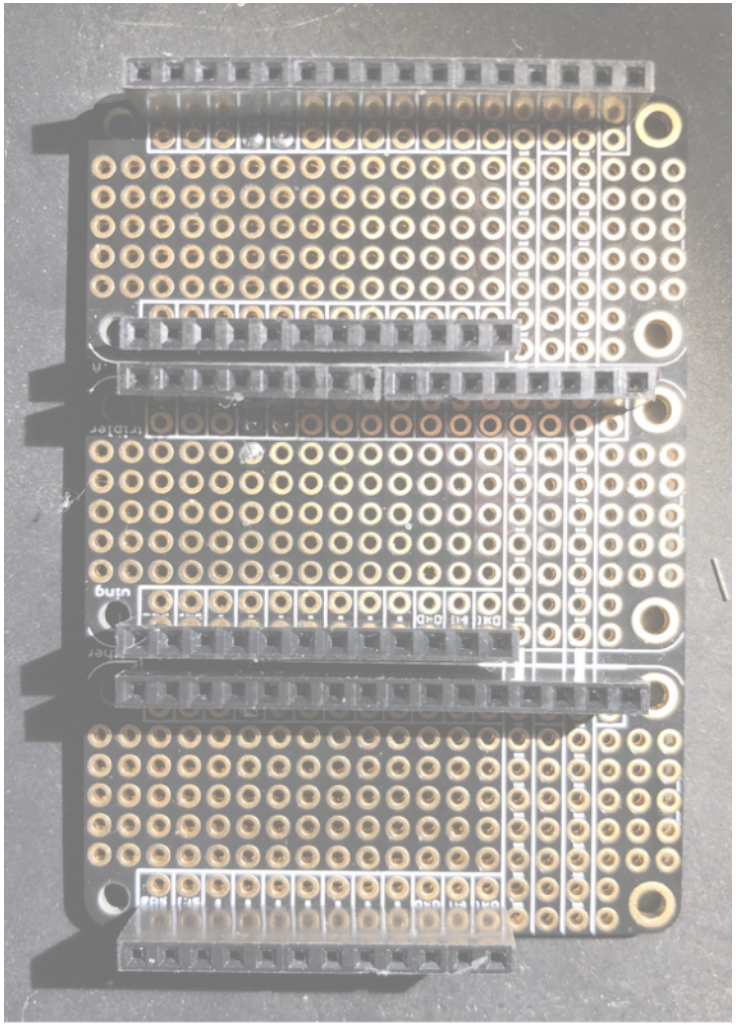
```
atlas@blah:~$ rfcat -r
'RfCat, the greatest thing since Frequency Hopping!'

Don't you wish this were a CLI!?  Sorry.  Maybe soon...
For now, enjoy the raw power of rflib, or write your own device-specific CLI!

currently your environment has an object called "d" for dongle.  this is how
you interact with the rfcat dongle, for :
    >>> d.ping()
    >>> d.setFreq(433000000)
    >>> d.setMdmModulation(MOD_ASK_OOK)
    >>> d.makePktFLEN(250)
    >>> d.RFxmit("HALLO")
    >>> d.RFrecv()
    >>> print d.reprRadioConfig()


In [1]: d.ping()
PING: 26 bytes transmitted, received: 'ABCDEFGHIJKLMNOPQRSTUVWXYZ' (0.027489 seconds)
PING: 26 bytes transmitted, received: 'ABCDEFGHIJKLMNOPQRSTUVWXYZ' (0.011954 seconds)
PING: 26 bytes transmitted, received: 'ABCDEFGHIJKLMNOPQRSTUVWXYZ' (0.012381 seconds)
PING: 26 bytes transmitted, received: 'ABCDEFGHIJKLMNOPQRSTUVWXYZ' (0.012189 seconds)
PING: 26 bytes transmitted, received: 'ABCDEFGHIJKLMNOPQRSTUVWXYZ' (0.012411 seconds)
PING: 26 bytes transmitted, received: 'ABCDEFGHIJKLMNOPQRSTUVWXYZ' (0.012139 seconds)
PING: 26 bytes transmitted, received: 'ABCDEFGHIJKLMNOPQRSTUVWXYZ' (0.012379 seconds)
PING: 26 bytes transmitted, received: 'ABCDEFGHIJKLMNOPQRSTUVWXYZ' (0.012392 seconds)
PING: 26 bytes transmitted, received: 'ABCDEFGHIJKLMNOPQRSTUVWXYZ' (0.011946 seconds)
PING: 26 bytes transmitted, received: 'ABCDEFGHIJKLMNOPQRSTUVWXYZ' (0.011591 seconds)
Out[1]: (10, 0, 0.13894200325012207)
```

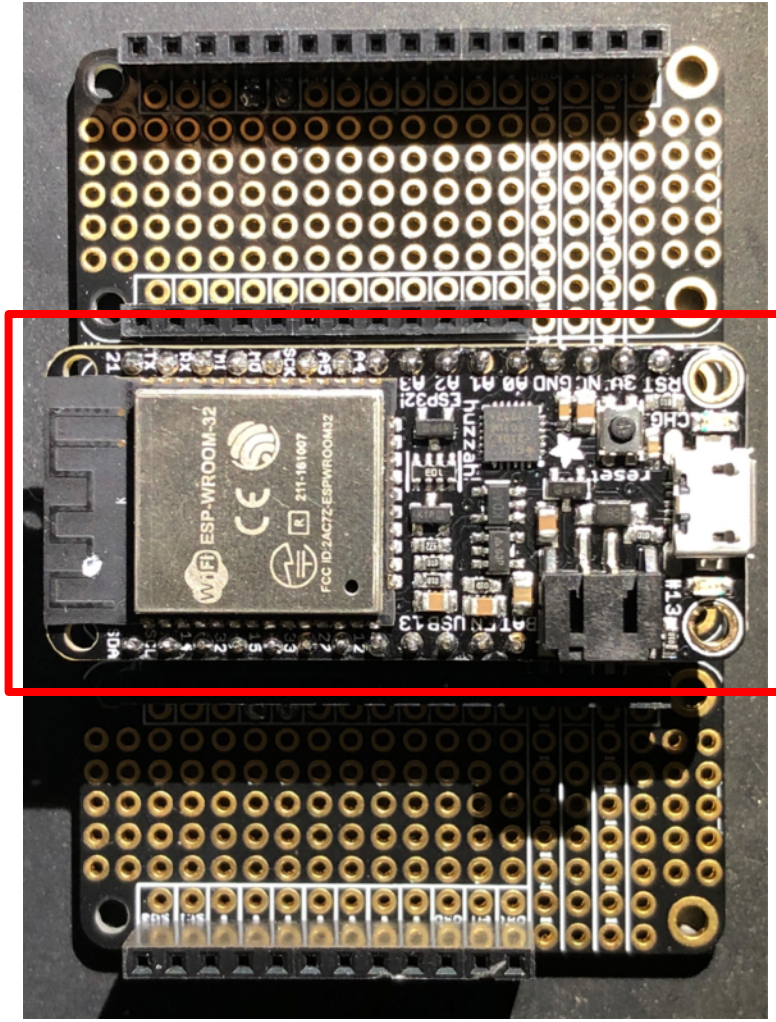
https://media.blackhat.com/bh-us-12/Briefings/Atlas/BH_US_12_Atlas_GHZ_Workshop_Slides.pdf



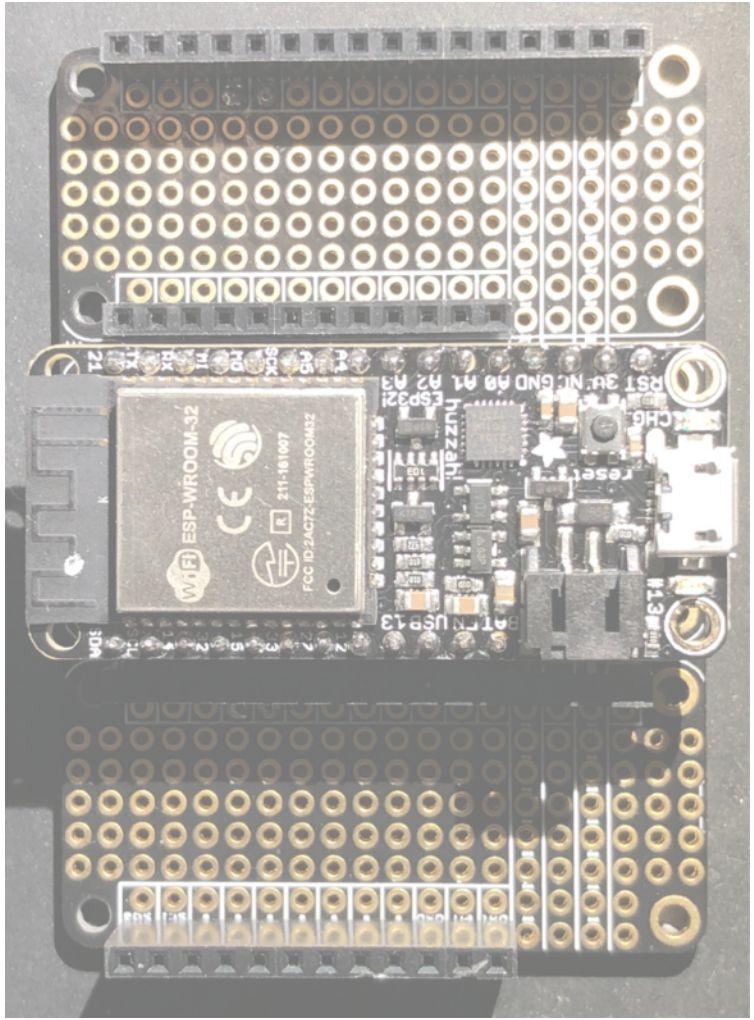
```
atlas@blah:~$ rfcat -r
'RfCat, the greatest thing since Frequency Hopping!'

Don't you wish this were a CLI!?  Sorry.  Maybe soon...
For now, enjoy the raw power of rflib, or write your own device-specific CLI!

currently your environment has an object called "d" for dongle.  this is how
you interact with the rfcat dongle, for :
    >>> d.ping()
    >>> d.setFreq(433000000)
    >>> d.setMdmModulation(MOD_ASK_OOK)
    >>> d.makePktFLEN(250)
    >>> d.RFxmit("HALLO")
    >>> d.RFrecv()
    >>> print d.reprRadioConfig()


In [1]: d.ping()
PING: 26 bytes transmitted, received: 'ABCDEFGHIJKLMNOPQRSTUVWXYZ' (0.027489 seconds)
PING: 26 bytes transmitted, received: 'ABCDEFGHIJKLMNOPQRSTUVWXYZ' (0.011954 seconds)
PING: 26 bytes transmitted, received: 'ABCDEFGHIJKLMNOPQRSTUVWXYZ' (0.012381 seconds)
PING: 26 bytes transmitted, received: 'ABCDEFGHIJKLMNOPQRSTUVWXYZ' (0.012189 seconds)
PING: 26 bytes transmitted, received: 'ABCDEFGHIJKLMNOPQRSTUVWXYZ' (0.012411 seconds)
PING: 26 bytes transmitted, received: 'ABCDEFGHIJKLMNOPQRSTUVWXYZ' (0.012139 seconds)
PING: 26 bytes transmitted, received: 'ABCDEFGHIJKLMNOPQRSTUVWXYZ' (0.012379 seconds)
PING: 26 bytes transmitted, received: 'ABCDEFGHIJKLMNOPQRSTUVWXYZ' (0.012392 seconds)
PING: 26 bytes transmitted, received: 'ABCDEFGHIJKLMNOPQRSTUVWXYZ' (0.011946 seconds)
PING: 26 bytes transmitted, received: 'ABCDEFGHIJKLMNOPQRSTUVWXYZ' (0.011591 seconds)
Out[1]: (10, 0, 0.13894200325012207)
```

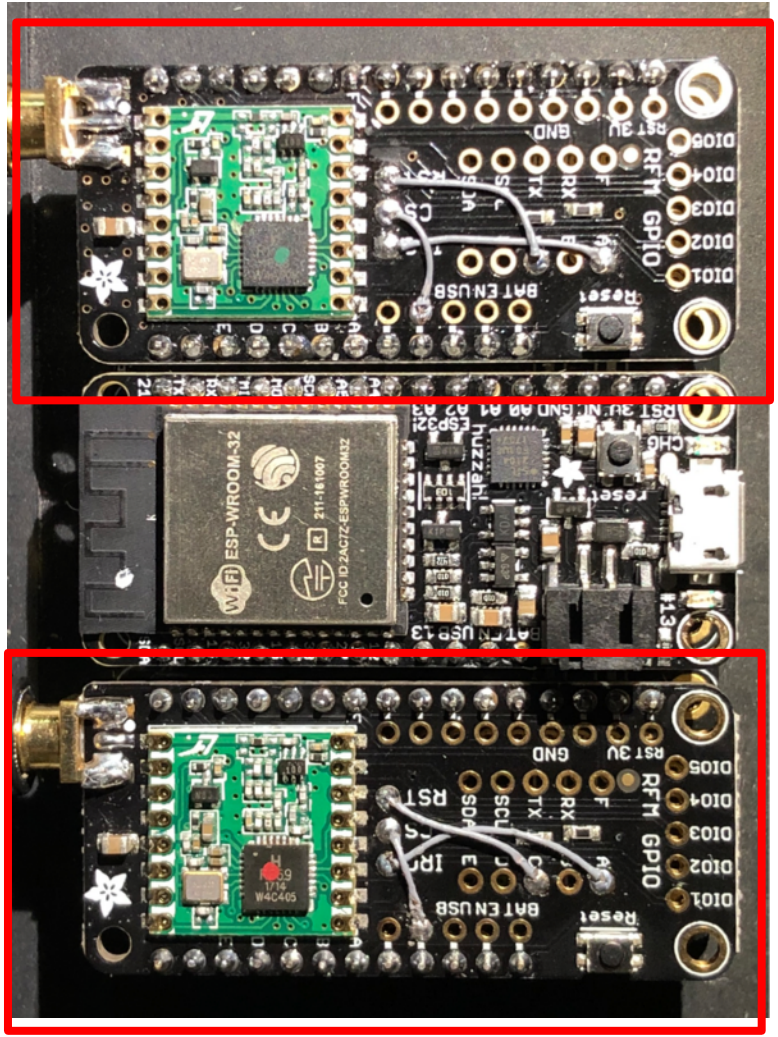


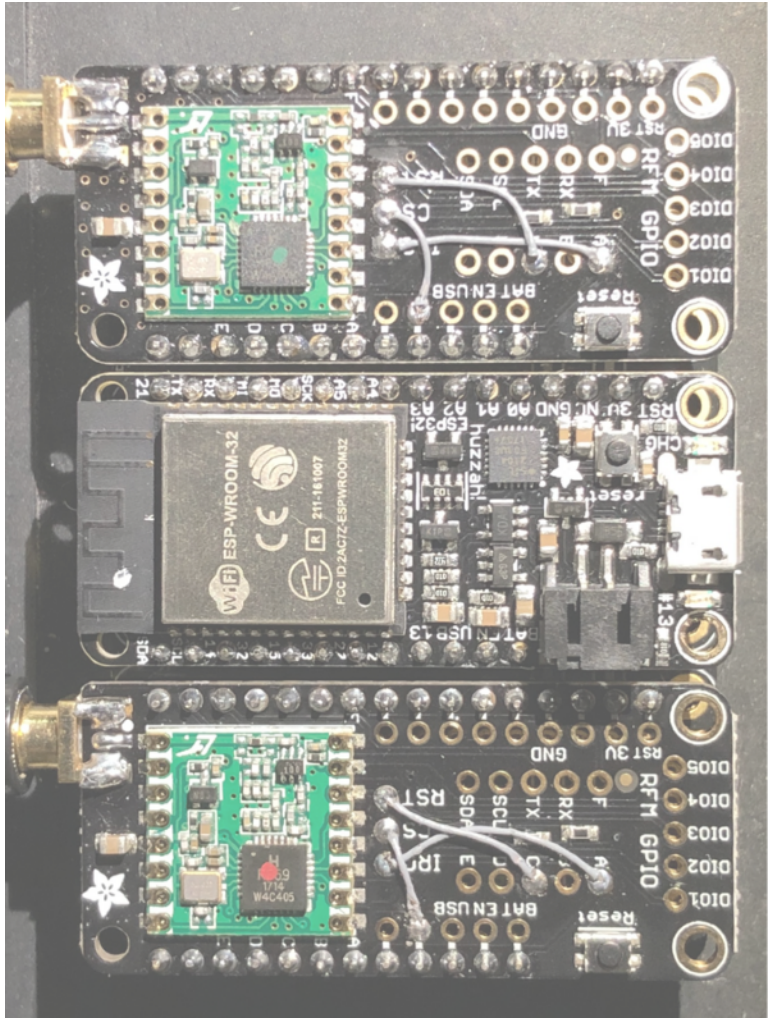




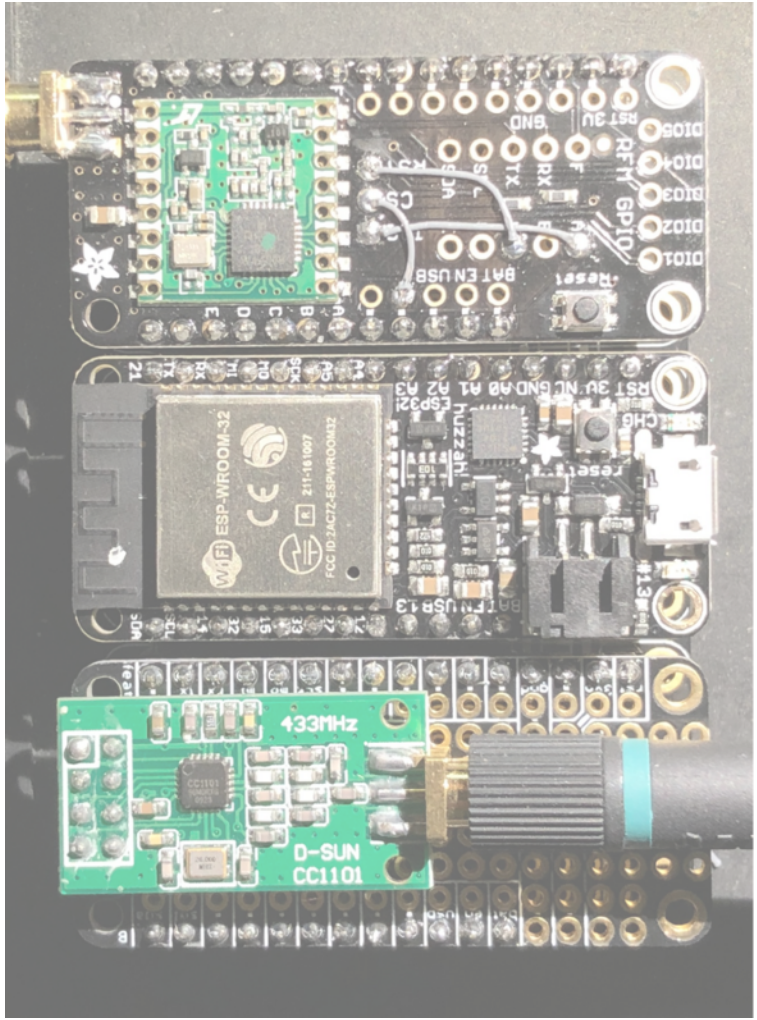
MCU:
ESP32

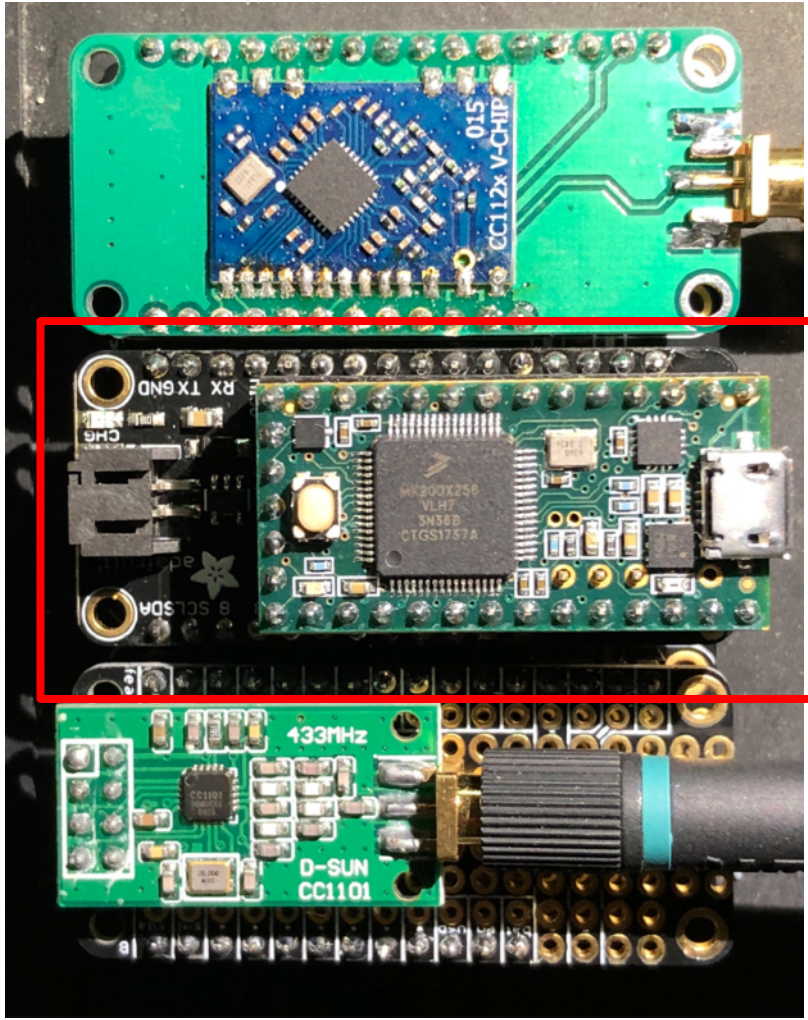


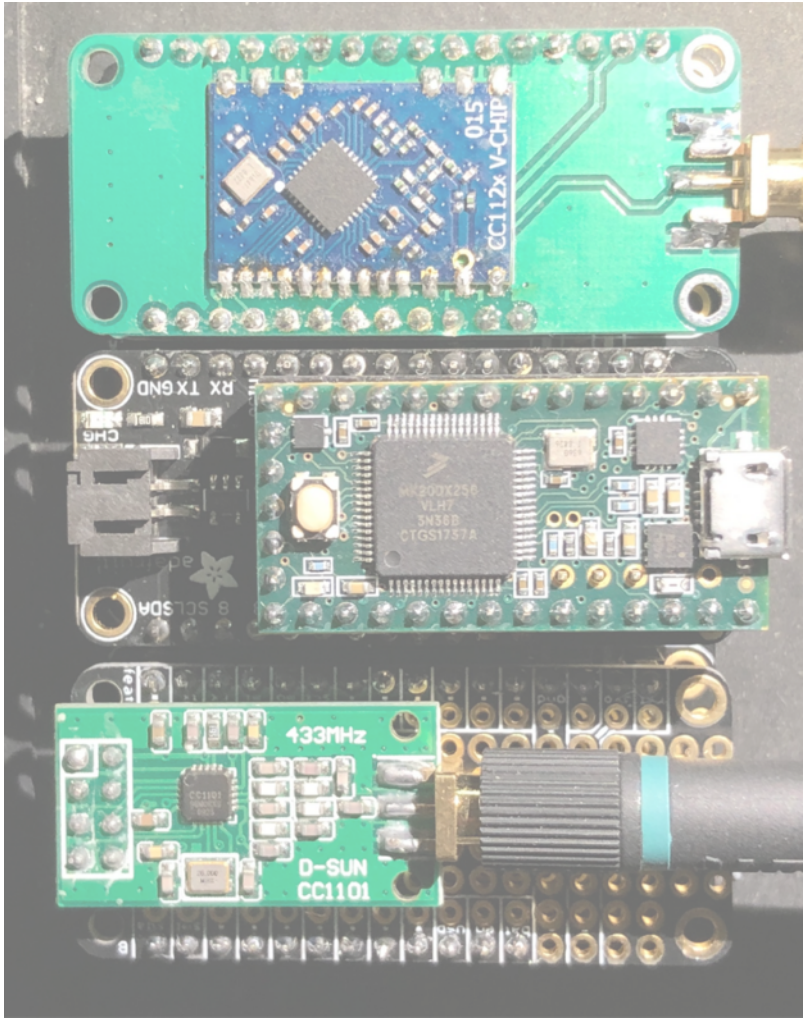


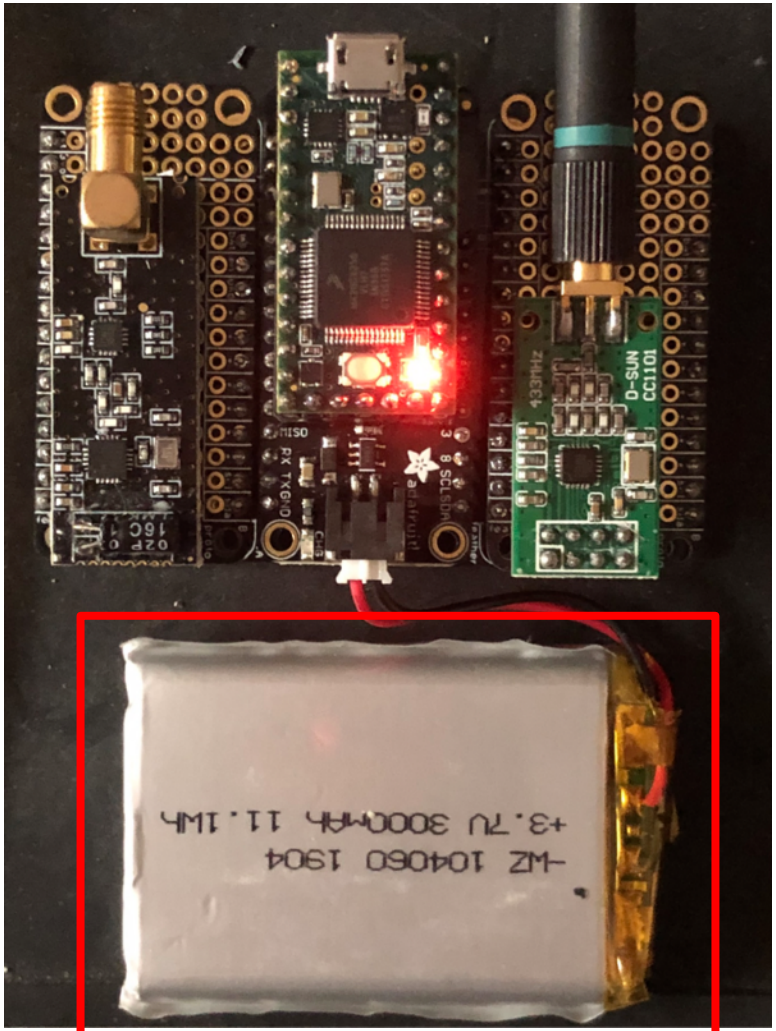

ESP-WROOM-32
RFM GPIO
BAT EN USB
Reset
Huzzah
ESP32
433MHz
D-SUN
CC1101

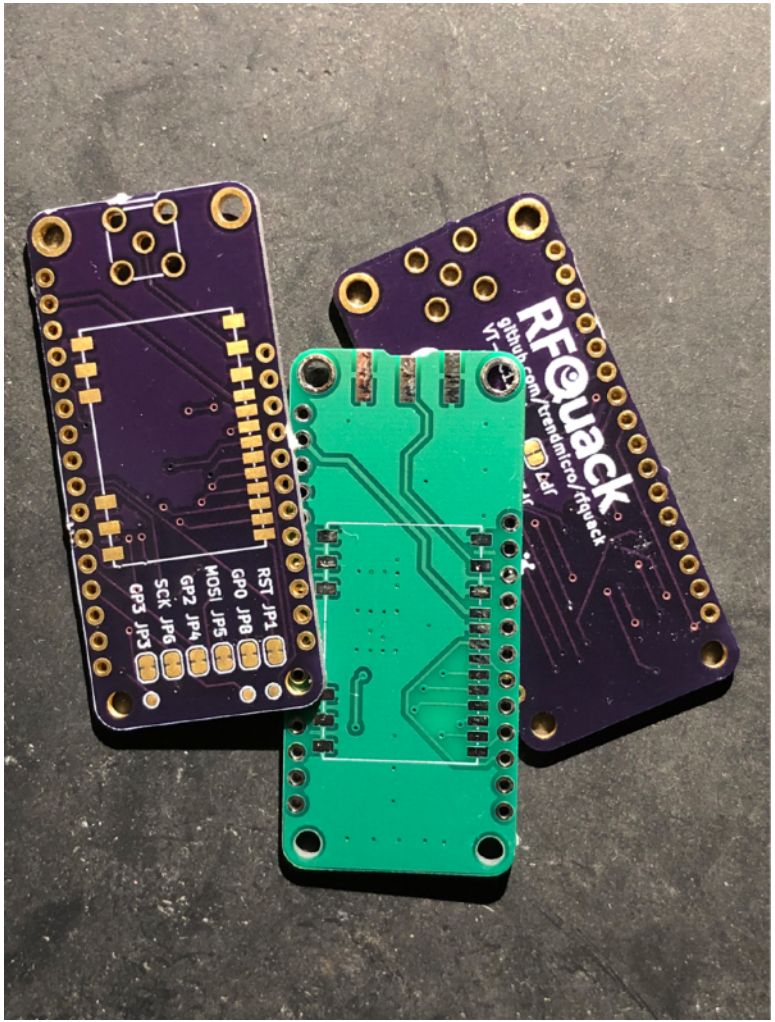
RFM GPIO
D105
D104
D103
D102
D101

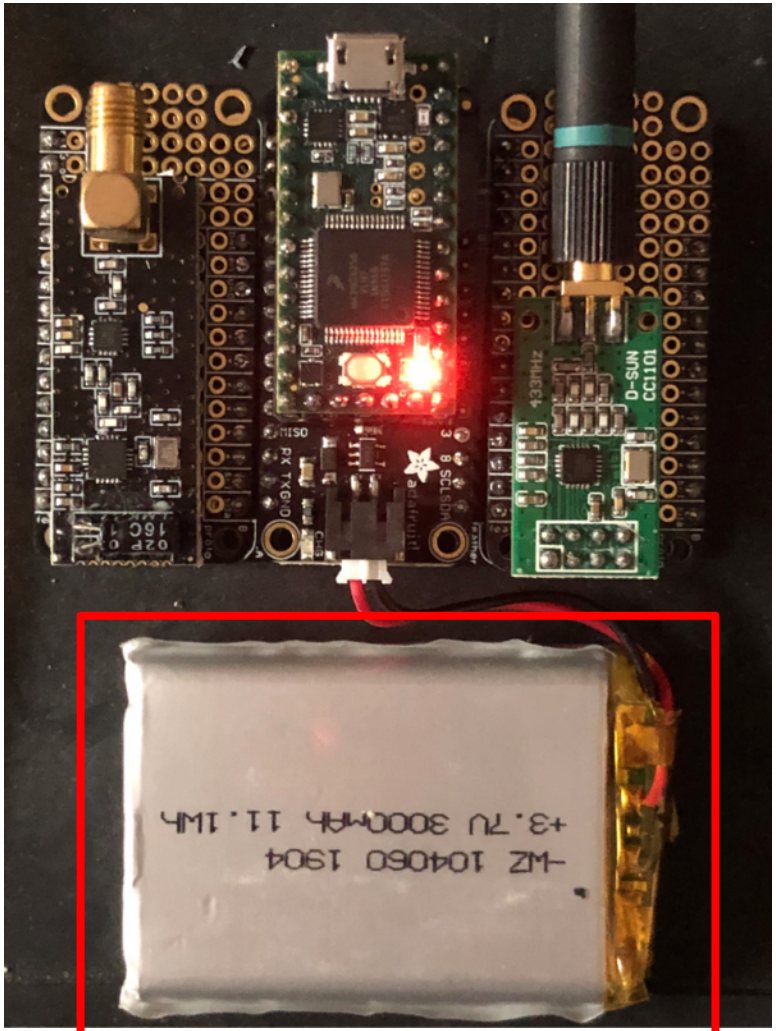

ESP-WROOM-32
433MHz
D-SUN
CC1101

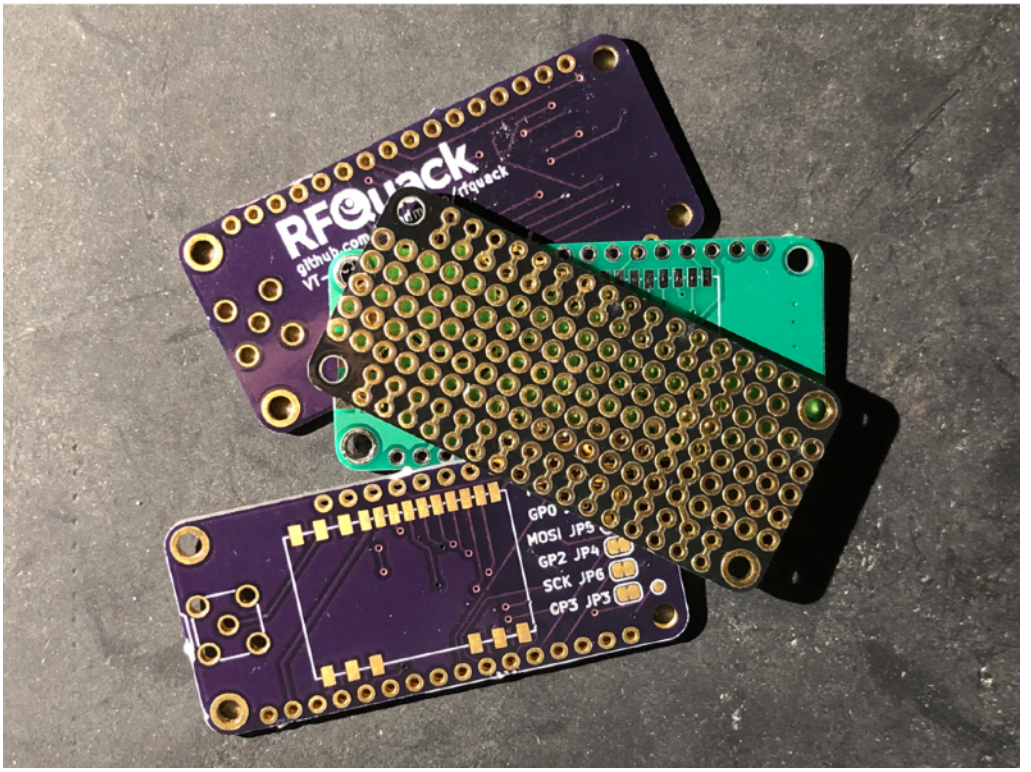

CC112x V-CHIP
433MHz
D-SUN
CC1101

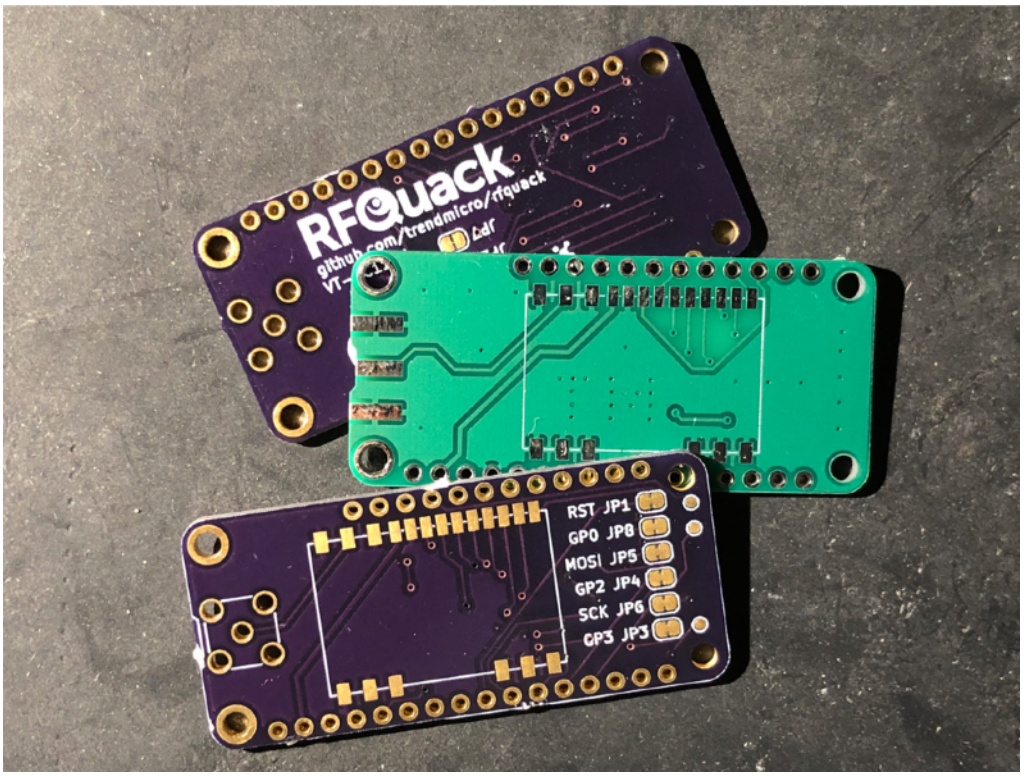

015
CC112x V-CHIP
RX TX GND
433MHz
D-SUN
CC1101

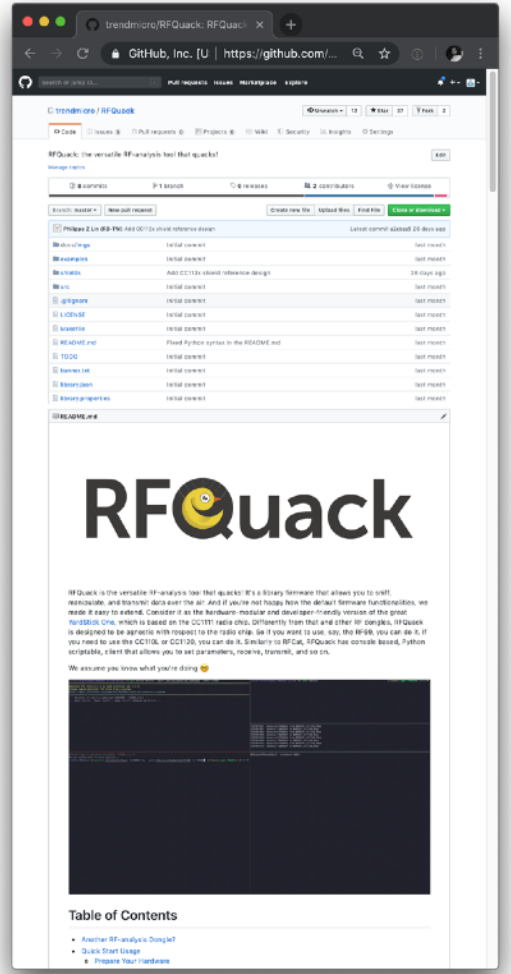

433MHz
D-SUN
CC1101


RFQuack
RST JP1
GP0 JP0
MOSI JP5
GP2 JP4
SCK JP6
GP3 JP3


D-SUN
CC1101
3 SCL SDA
RX TX GND


GP0 -
MOSI JP5
GP2 JP4
SCK JP6
GP3 JP3


RFQuack
RST JP1
GP0 JP8
MOSI JP5
GP2 JP4
SCK JP6
GP3 JP3



https://github.com/trendmicro/RFQuack

- receive
- sniff
- filter packets
- manipulate packets on the fly
- re-transmit (modified packets)
- low-level register access

- ...clean protobuf API

DEMO?

References

- high-level blog post: https://is.gd/rfhw101
- detailed tech brief: https://is.gd/rfhw101pdf

Reverse engineering di protocolli radio proprietari: dalle basi al design di un ricetrasmettitore in hardware

Federico Maggi, @phretor
https://maggi.cc - https://ggad.it

TREND MICRO™ | research

HACK IN BO® Winter 2019 Edition
13ª EDIZIONE