



How to hack the drone

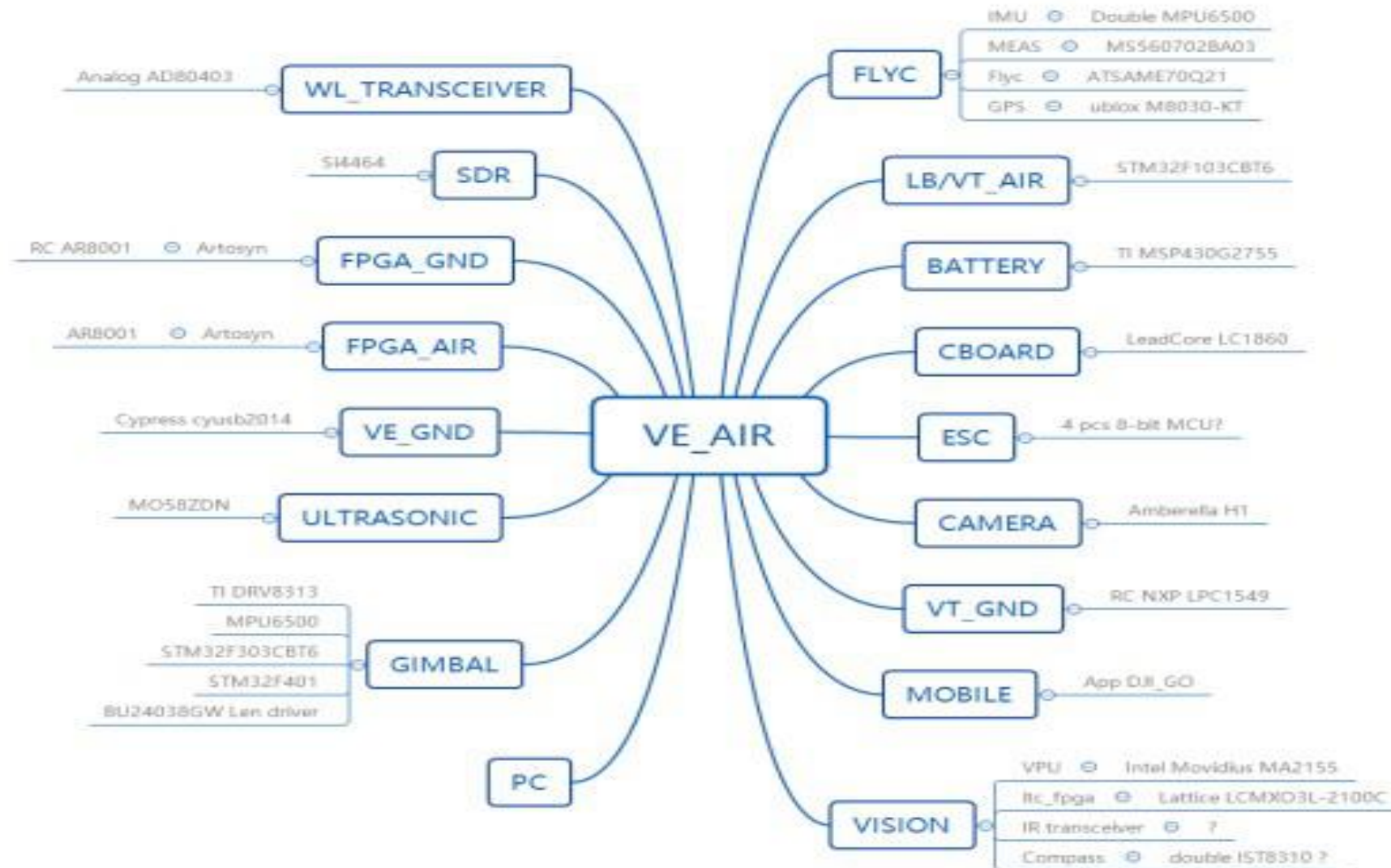
Xie Jun 2017.11.18

UAV is a complicated systematic project

DJI UAV



DJI P4P Architecture



DJI Architecture - Communication between modules

- Two bytes of the communication source or destination address

Subsystem Number functions Number

E.g 03 He represents flight control, 06 Show 6 Chant function

> A total of no more than 32 Sub-systems

> Channel mode

> local, IP, WL, UART, I2C, SPI, CAN, ADB

> HPI, USB, IAP2

> letter of agreement

> Logic

> V0

> V1

> NAL

> MAVLink

```
; "whoami" 00
; "camera" 01
; "mobile" 02
; "flight" 03
; "gimbal" 04
; "cboard" 05
; "rc" 06
; "network" 07
; "ve_air" 08
; "vt_air" 09
; "pc" 0a
; "battery" 0b
; "esc" 0c
; "ve_gnd" 0d
; "vt_gnd" 0e
; "s_to_p_air" 0f
; "s_to_p_gnd" 10
; "mvision" 0x11
; "bvision" 0x12
; "fpga_air" 0x13
; "fpga_gnd" 0x14
; "simulator" 0x15
; "null"
; "null"
; "null"
; "null"
; "mavlink" 0x1a
; "null"
; "glass" 0x1c
; "blackbox" 0x1d
; "test" 0x1e
; "all" 0x1f
```

```
0100 camera
0200 mobile
0400 gimbal
0500 cboard
0801 dji_sys
0802 ma2155
0803 ltc_fpga
0804 ultrasonic
0805 dji_vision
0806 dji_decoding
0807 test_diag
0a00 pc con
0a02 firmware update from pc
1107 ma2155 vision
1105 dji_flight for NFZ
0300 fly control
0301
0302
0303
0304
0305
0306
0900 LightBridge
0905 download service
0b00 battery
0c00 ESC 1
0c01 ESC 2
0c02 ESC 3
0c03 ESC 4
0d00 RC cyusb
0e00 RC LPC1549
1f00 all
```


DJI Architecture - Communication between modules

- letter of agreement Logic & V1

message v1 format

Magic Header 1byte • 0x55

Packet Len 10bits -> less than 0x400

version 1byte & 4 -> 4 in P4 & P4P

CRC8 cksum 1 byte -> crc8 (header [0: 3])

Seq 2bytes -> random

src ID 1byte -> 0A • 0A00

dst ID 1byte -> 0E -> 0E00

Attr ID 1byte ->

cmd ID 2bytes -> 00 01 version request

sub_cmd ID 1byte optional

body len 2bytes optional

body few bytes optional

crc16 cksum 2bytes -> crc16 (pkt [- 2])

```
55 0D 04 33 0A 0E 13 27 40 00 01 16 72 .....U..3...'@...r
55 2C 04 36 0E 0A 13 27 80 00 01 00 10 50 34 5F ...U,.6...'€....P4_
50 56 32 00 00 00 00 00 00 00 00 00 06 03 01 ...PV2.....
03 02 03 02 05 43 02 00 00 00 8F 8B .....C.....e
```

DJI Architecture - Communication between modules

- letter of agreement Logic & V1

message Logic Format

Magic header 4bytes -> 21 12 ad de

src ID 2bytes ->

dst ID 2bytes ->

Seq 2bytes ->

Attr ID 1byte ->

CMD ID 2bytes ->

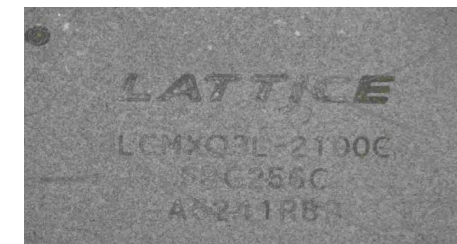
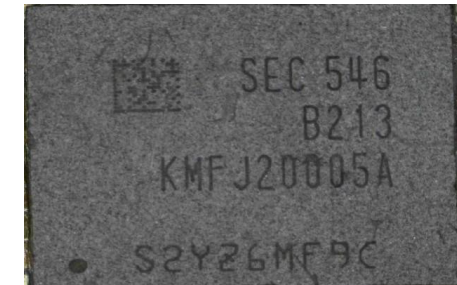
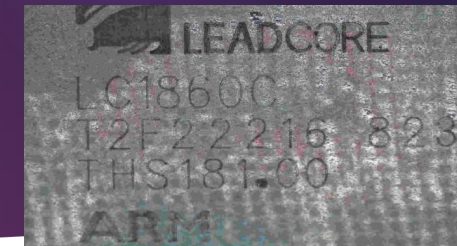
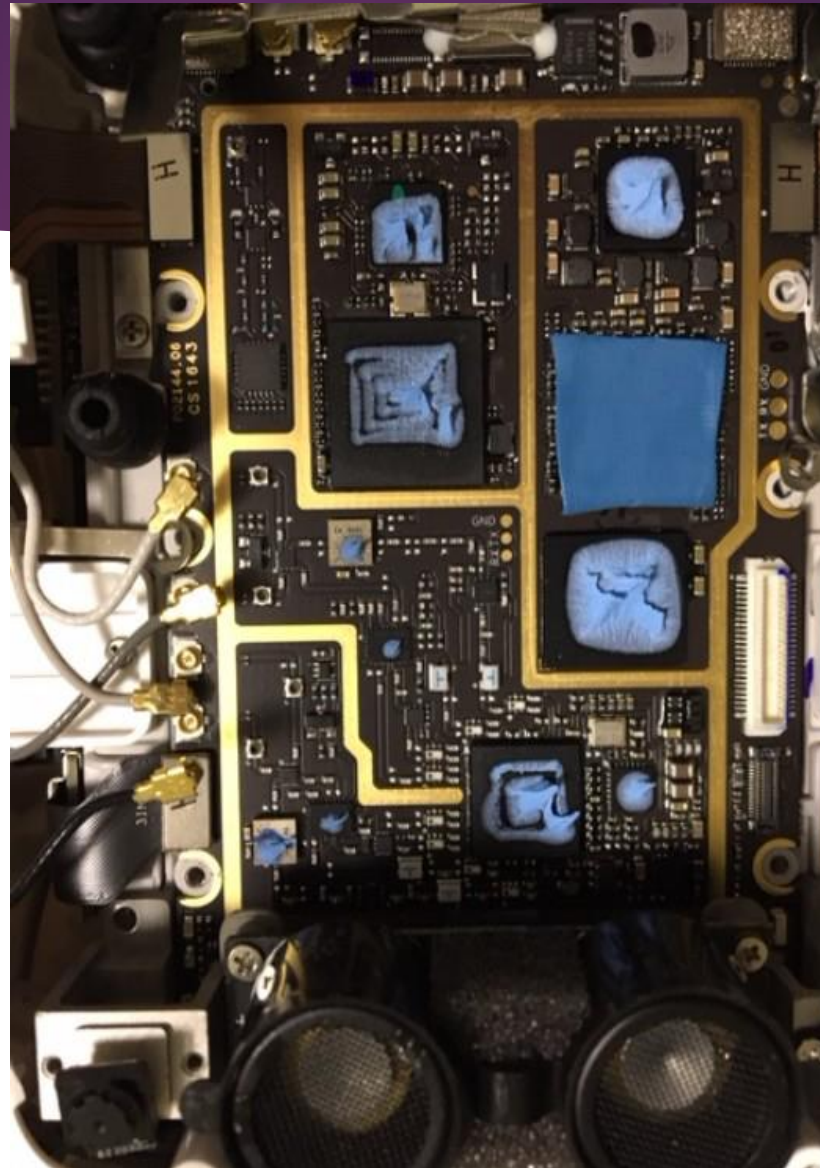
body few bytes ->

pkt len 2bytes -> packet len-6

```
def gen_host(d):  
    c=(d>>5)|((d&0x1f)<<8)  
    return c  
  
gen_host(0xf1)==0x1107  
gen_host(0x09)==0x0900
```


CenterBoard

- CenterBoard MCU LC1860
- Vision MA2155 + Lattice LCMXO3L2100C
- Memory & Storage
Samsung
eMCP (eMMC + DRAM)
KMFJ20005A 4GB
- SiliCon LABS Si4464



Root UAV

why would root UAV?

UAV research more convenient, easy to study other target modules

CenterBoard MCU LC1860 Embedded Systems linux , With adb The

default is to open the key scripts Start_dji_system.sh , adb_en.sh

```
debug=false
grep production /proc/cmdline >> /dev/null
if [ $? != 0 ]; then
    debug=true # engineering version, enable adb by default
else
    cmdline='cat /proc/cmdline'
    temp=${cmdline##*board_sn=}
    board=${temp%% *}
    in_whitelist.sh $board
    if [ $? == 0 ]; then
        debug=true
    fi
fi

if $debug; then
    /system/bin/adb_en.sh
else
    setprop sys.usb.config rndis,mass_storage,bulk,acm
fi
```

how root ?

1. Software vulnerability to do adb_en.sh script
2. If you can modify start_dji_system.sh script

"Debug = true" Can be reached root purpose

```
#!/system/bin/sh

level=$1
: ${level:=NonSecurePrivilege}

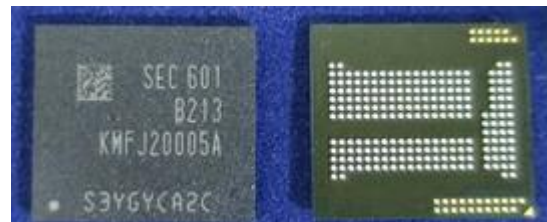
# mark debug enable
mkdir -p /tmp/dji
echo $level > /tmp/dji/secure_debug

# init adb device serial
if [ -f /data/dji/cfg/adb_serial ]; then
    serial=`cat /data/dji/cfg/adb_serial`
    busybox printf "$serial" > /sys/class/android_usb/android0/iSerial
fi

setprop service.adb.root 1
setprop service.adb.tcp.port -1
setprop sys.usb.config rndis,mass_storage,bulk,acm,adb
busybox devmem 0xe10093d0 8 0x40 #enable uart
sleep 1
busybox udhcpd
```

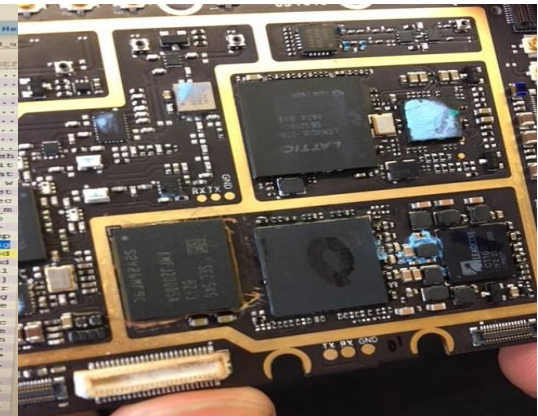
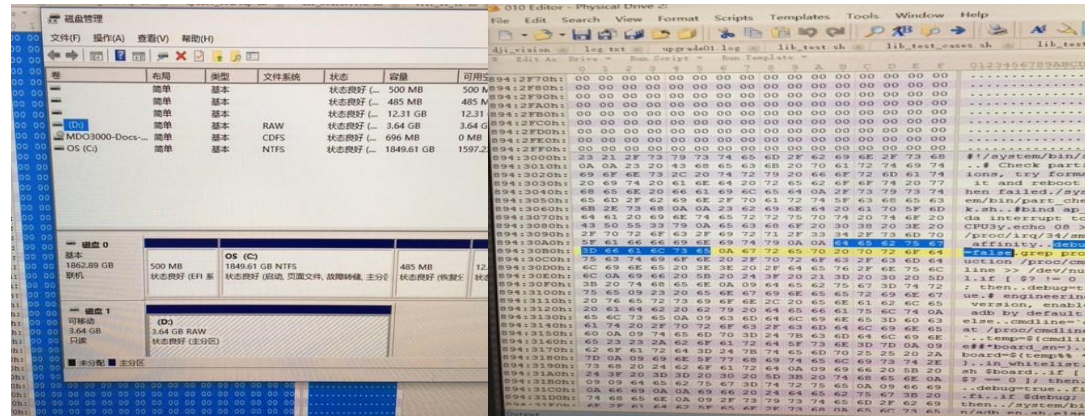
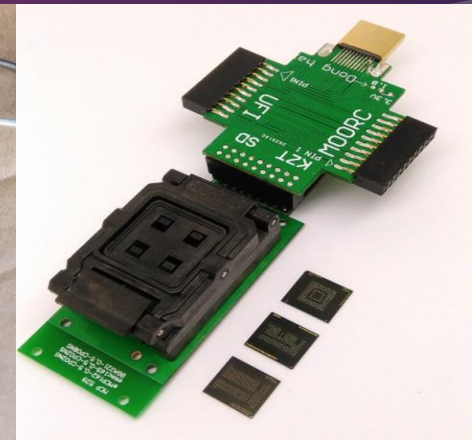
Root UAV

- By modifying start_dji_system.sh Script reach root effect
- More generic root The method requires rigid-flex
- The goal is to modify the contents of memory inside



Root UAV

- The blowing air gun eMCP
- eMMC The card reader reads Raw data
- Find the right partition file storage
- Ext4 Mounting system Partition
- modify start_dji_system.sh file
- System img Write back Raw Data file
- eMMC Readers write back eMCP
- eMCP Chip soldered back seat



Root UAV

- finally

```

CPU architecture: 7
CPU variant      : 0x0
CPU part         : 0xc07
CPU revision     : 5

processor        : 3
model name       : ARMv7 Processor rev 5 (v7l)
Processor        : ARMv7 Processor rev 5 (v7l)
BogoMIPS         : 26.00
Features         : swp half thumb fastmult vfp edsp neon vfpv3 t
CPU implementer  : 0x41
CPU architecture: 7
CPU variant      : 0x0
CPU part         : 0xc07
CPU revision     : 5

processor        : 4
model name       : ARMv7 Processor rev 5 (v7l)
Processor        : ARMv7 Processor rev 5 (v7l)
BogoMIPS         : 26.00
Features         : swp half thumb fastmult vfp edsp neon vfpv3 t
CPU implementer  : 0x41
CPU architecture: 7
CPU variant      : 0x0
CPU part         : 0xc07
CPU revision     : 5

Hardware         : Leadcore Innopower
Revision         : 0000
Serial          : 0000000000000000
root@wm330_dz_vp0001_v5:/ # df
Filesystem      Size      Used      Free      Blksize
/dev            8.0M      128.0K      7.9M      4096
/tmp            32.0M      12.0K      32.0M      4096
/var            2.0M      12.0K      2.0M      4096
/ftp            1024.0K      0.0K      1024.0K      4096
/amt            11.7M      68.0K      11.7M      4096
/vendor         59.0M      6.8M      52.2M      4096
/system         122.0M      96.9M      25.1M      4096
/data           1.1G      97.3M      1018.6M      4096
/blackbox       1.1G      97.0M      1018.9M      4096
/cache          1.9G      1.2G      1018.9M      4096
/ftp/upgrade    248.0M      55.0M      193.0M      4096
/ftp/blackbox   1.1G      97.0M      1018.9M      4096
/tmp/cam_storage 1.9G      1.2G      796.1M      4096
root@wm330_dz_vp0001_v5:/ #

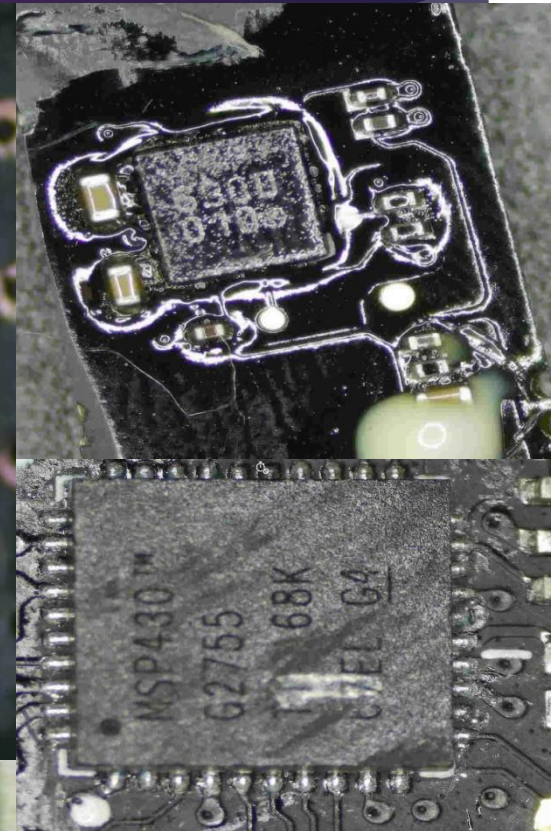
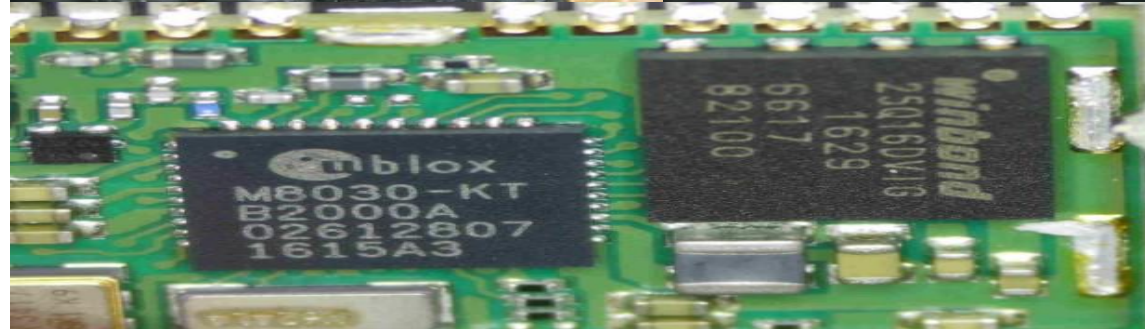
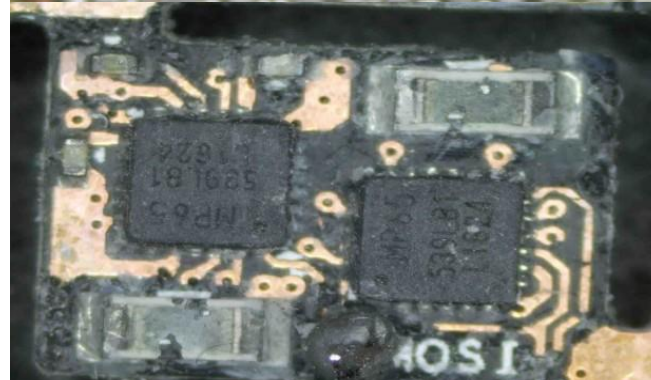
taps /dev/pts/depts rw,relatime,mode=755 0 0
devpts /dev/pts/depts rw,relatime,mode=600 0 0
proc /proc rw,relatime 0 0
sysfs /sys sysfs rw,relatime 0 0
tmpfs /tmp tmpfs rw,relatime,size=32768k 0 0
tmpfs /var tmpfs rw,relatime,size=2048k 0 0
tmpfs /ftp tmpfs rw,relatime,size=1024k 0 0
/dev/block/platform/comp-mmc.1/by-name/amt /amt ext4 ro,relatime,data=ordered 0 0
/dev/block/platform/comp-mmc.1/by-name/vendor /vendor ext4 ro,relatime,data=ordered 0 0
/dev/block/platform/comp-mmc.1/by-name/userdata /system ext4 rw,relatime,data=ordered 0 0
/dev/block/platform/comp-mmc.1/by-name/blackbox /blackbox ext4 rw,relatime,data=ordered 0 0
/dev/block/platform/comp-mmc.1/by-name/cache /cache ext4 rw,relatime,data=ordered 0 0
/dev/block/platform/comp-mmc.1/by-name/userdata /ftp/upgrade ext4 rw,relatime,data=ordered 0 0
/dev/block/platform/comp-mmc.1/by-name/blackbox /ftp/blackbox ext4 rw,relatime,data=ordered 0 0
/dev/block/sda1 /tmp/cam_storage vfat rw,relatime,nosk=0000,dmask=0000,allow_utime=0022,codpage=437,iocharset=
root@wm330_dz_vp0001_v5:/ # df
Filesystem      Size      Used      Free      Blksize
/dev            8.0M      128.0K      7.9M      4096
/tmp            32.0M      12.0K      32.0M      4096
/var            2.0M      12.0K      2.0M      4096
/ftp            1024.0K      0.0K      1024.0K      4096
/amt            11.7M      68.0K      11.7M      4096
/vendor         59.0M      6.8M      52.2M      4096
/system         122.0M      96.9M      25.1M      4096
/data           1.1G      97.3M      1018.6M      4096
/blackbox       1.9G      993.6M      990.2M      4096
/cache          248.0M      55.0M      193.0M      4096
/ftp/upgrade    1.1G      97.3M      1018.6M      4096
/ftp/blackbox   1.9G      993.6M      990.2M      4096
/tmp/cam_storage 14.9G      10.9G      4.0G      32768
root@wm330_dz_vp0001_v5:/ # busybox uname -a
Linux localhost 3.10.62 #1 SMP PREEMPT Fri Nov 4 11:48:41 CST 2016 armv7l GNU/Linux
root@wm330_dz_vp0001_v5:/ #

Proto Recv-Q Send-Q Local Address          Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:0.8905        0.0.0.0:*               LISTEN      204/djnl_monitor
tcp        0      0 0.0.0.0:0.8906        0.0.0.0:*               LISTEN      206/djnl_sys
tcp        0      0 0.0.0.0:0.8907        0.0.0.0:*               LISTEN      208/djnl_encoding
tcp        0      0 0.0.0.0:0.8908        0.0.0.0:*               LISTEN      210/djnl_vision
tcp        0      0 0.127.0.0:1.5837      0.0.0.0:*               LISTEN      307/oddb
tcp        0      0 0.192.168.42:2.21    0.0.0.0:*               LISTEN      307/oddb
netstat: /proc/net/tcp6: No such file or directory
udp        0      0 0.0.0.0:0.67         0.0.0.0:*               LISTEN      179/busybox
udp        0      0 0.0.0.0:0.67         0.0.0.0:*               LISTEN      325/busybox
netstat: /proc/net/udp6: No such file or directory
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags       Type       State           I-Node PID/Program name      Path
unix 2      [ ]         DGRAM      LISTENING      2170 206/djnl_sys           @/duss/mb/Bc1f00
unix 2      [ ACC ]     STREAM     LISTENING      2188 1/init                 /dev/socket/property_ser
unix 2      [ ]         DGRAM      2168 206/djnl_sys           @/duss/mb/Bc800
unix 2      [ ]         DGRAM      2167 206/djnl_sys           @/duss/mb/Bc800
unix 2      [ ]         DGRAM      2166 206/djnl_sys           @/duss/mb/Bc803
unix 2      [ ]         DGRAM      2165 206/djnl_sys           @/duss/mb/Bc802
unix 2      [ ]         DGRAM      2162 208/djnl_encoding     @/duss/mb/Bx801
unix 2      [ ]         DGRAM      2163 210/djnl_vision       @/duss/mb/Bx800
unix 2      [ ]         DGRAM      2174 206/djnl_sys           @/duss/mb/Bx107
unix 2      [ ]         DGRAM      3124 204/djnl_monitor      @/duss/mb/Bx002
unix 2      [ ACC ]     STREAM     LISTENING      3125 211/debugger          @/duss/mb/Bx002
unix 2      [ ACC ]     STREAM     LISTENING      3156 307/oddb              @android:debugger
unix 3      [ ]         STREAM     CONNECTED      2169 206/djnl_sys           @jdmp-control
unix 3      [ ]         STREAM     CONNECTED      2113 1/init                 @/duss/mb/Bx00
unix 3      [ ]         STREAM     CONNECTED      60354 307/oddb
unix 3      [ ]         STREAM     CONNECTED      3154 307/oddb
unix 3      [ ]         STREAM     CONNECTED      2114 1/init
unix 2      [ ]         DGRAM      60353 307/oddb
unix 2      [ ]         DGRAM      4215 206/djnl_sys
unix 2      [ ]         STREAM     CONNECTED      3120 208/djnl_encoding
unix 2      [ ]         DGRAM      3157 307/oddb
unix 2      [ ]         DGRAM      2174 210/djnl_vision
unix 2      [ ]         STREAM     CONNECTED      3123 204/djnl_monitor
unix 3      [ ]         STREAM     CONNECTED      3158 307/oddb
root@wm330_dz_vp0001_v5:/ #

```

Flight Control System

- Flight Control MCU Atmel ATSAME 70Q21
- IMU MP6500 (Gyroscope + accelerometer)
- Barometer MEAS
MS560702BA03
- Ublox GPS Module
- Double IST8310 Compass Module
- Smart Power
- ESC ESC



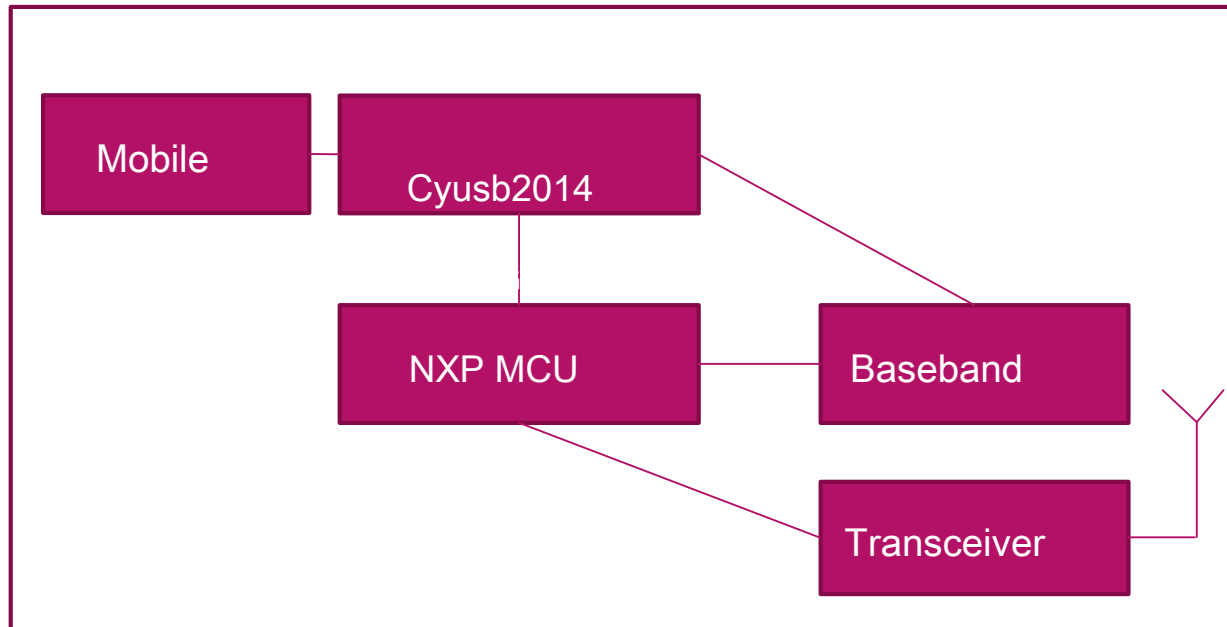
visual system

- MA2155 Depth visual processing
 - And the front obstacle recognition ranging
 - Character, attitude, water, ROI Recognition
- Binocular infrared obstacle avoidance
 - Infrared about recognition
- Ultrasonic wave
 - Below the obstacle detection

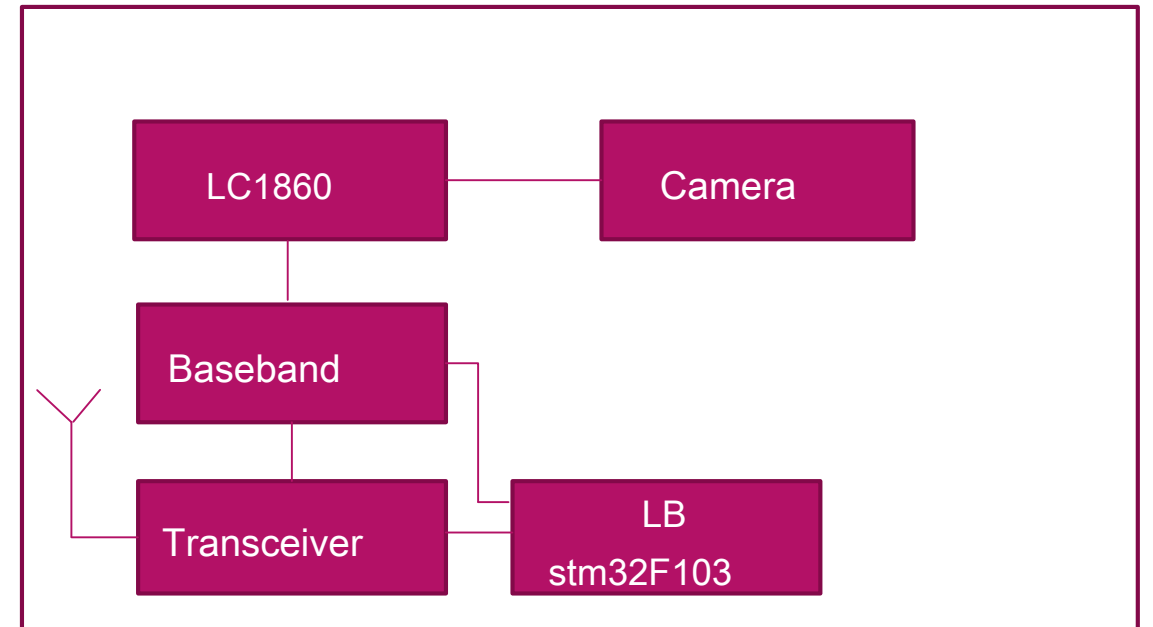


Wireless communication system architecture

RC



Aircraft



Wireless communication system architecture

- FIG NC & passage downstream channel
- OFDM Broadband transmission
- 1Mhz & 10Mhz bandwidth
- RC 1Tx & 2Rx signal path channel
- Air 1Tx & 2Rx signal path channel
- Transceiver AD80403 SPI config same as Ad9361
- CNC channel 2.4G 24 Hopping sequence, 5.8G 12 Hopping sequence
- CNC channel 2.4G 45 Frequency points, 5.8G 42 Frequency points
- Each switching frequency interval 14ms , 1s Switch 71 Frequency points

Operating Frequencies		
Device operates within approved frequencies overlapping with the following cellular bands: LTE 255, Unlicensed NII-3 DOWN LTE 46, TD Unlicensed DOWN		
Frequency Range	Power Output	Rule Parts
2.404-2.4768 GHz	566 mW	15C
5.727-5.8213 GHz	175 mW	15E



Wireless communication system architecture

- Pair & link
- The pairing code RC MCU ID generate
- by RC ID Hopping sequence generation

```
freq hop seed generation
4pro type==3

a=crc8(a1,4,0x33)
a1=[0xa7,0x9f,0x4e,0x09],rc id gened
```

```
table_58[1,5,0x0b,0x0d,0x11,0x13,0x17,0x19,0x1d,0x1f,0x25,0x29]
table_24[1,2,4,7,8,0x0b,0x0d,0x0e,0x10,0x11,0x13,0x16,0x17,0x1a,0x1c,0x1d,0x1f,0x20,0x22,0x25,0x26,0x29,0x2b,0x2c]
```

```
if band==2
    b=a%0x0c
    c=table_58[b]
if band==0
    b=a%0x18
    c=table_24[b]
init_seed=c
```

```
if band==2 and type==3
    hops=0x2a
if band==0 and type==3
    hops=0x2d
```

RC id generation algorithm

IAP_chip_ReadUID get 16 bytes

b1=crc8(uid,0x77)

b2=crc16(uid,0x3692)

b3=xor(uid,)

RC_id=[b2[0:1],b1,b3]

all of 5.8ghz freqz tx hop list

```
1
['5732.0', '5734.0', '5736.0', '5738.0', '5741.0', '5743.0', '5745.0', '5748.0', '5750.0', '5752.0', '5755.0', '5757.0', '5759.0', '5761.0', '5764.0', '5766.0', '5768.0', '5771.0', '5773.0', '5775.0', '5778.0',
'5780.0', '5782.0', '5784.0', '5787.0', '5789.0', '5791.0', '5794.0', '5796.0', '5798.0', '5801.0', '5803.0', '5805.0', '5807.0', '5810.0', '5812.0', '5814.0', '5817.0', '5819.0', '5821.0', '5727.0', '5729.0']
5
['5750.0', '5761.0', '5773.0', '5784.0', '5796.0', '5807.0', '5819.0', '5734.0', '5745.0', '5757.0', '5768.0', '5780.0', '5791.0', '5803.0', '5814.0', '5729.0', '5741.0', '5752.0', '5764.0', '5775.0', '5787.0',
'5798.0', '5810.0', '5821.0', '5736.0', '5748.0', '5759.0', '5771.0', '5782.0', '5794.0', '5805.0', '5817.0', '5732.0', '5743.0', '5755.0', '5766.0', '5778.0', '5789.0', '5801.0', '5812.0', '5727.0', '5738.0']
11
['5778.0', '5803.0', '5732.0', '5757.0', '5782.0', '5807.0', '5736.0', '5761.0', '5787.0', '5812.0', '5741.0', '5766.0', '5791.0', '5817.0', '5745.0', '5771.0', '5796.0', '5821.0', '5750.0', '5775.0', '5801.0',
'5729.0', '5755.0', '5780.0', '5805.0', '5734.0', '5759.0', '5784.0', '5810.0', '5738.0', '5764.0', '5789.0', '5814.0', '5743.0', '5768.0', '5794.0', '5819.0', '5748.0', '5773.0', '5798.0', '5727.0', '5752.0']
13
['5787.0', '5817.0', '5750.0', '5780.0', '5810.0', '5743.0', '5773.0', '5803.0', '5736.0', '5766.0', '5796.0', '5729.0', '5759.0', '5789.0', '5819.0', '5752.0', '5782.0', '5812.0', '5745.0', '5775.0', '5805.0',
'5738.0', '5768.0', '5798.0', '5732.0', '5761.0', '5791.0', '5821.0', '5755.0', '5784.0', '5814.0', '5748.0', '5778.0', '5807.0', '5741.0', '5771.0', '5801.0', '5734.0', '5764.0', '5794.0', '5727.0', '5757.0']
17
['5805.0', '5748.0', '5787.0', '5729.0', '5768.0', '5807.0', '5750.0', '5789.0', '5732.0', '5771.0', '5810.0', '5752.0', '5791.0', '5734.0', '5773.0', '5812.0', '5755.0', '5794.0', '5736.0', '5775.0', '5814.0',
'5757.0', '5796.0', '5738.0', '5778.0', '5817.0', '5759.0', '5798.0', '5741.0', '5780.0', '5819.0', '5761.0', '5801.0', '5743.0', '5782.0', '5821.0', '5764.0', '5803.0', '5745.0', '5784.0', '5727.0', '5766.0']
19
['5814.0', '5761.0', '5805.0', '5752.0', '5796.0', '5743.0', '5787.0', '5734.0', '5778.0', '5821.0', '5768.0', '5812.0', '5759.0', '5803.0', '5750.0', '5794.0', '5741.0', '5784.0', '5732.0', '5775.0', '5819.0',
'5766.0', '5810.0', '5757.0', '5801.0', '5748.0', '5791.0', '5738.0', '5782.0', '5729.0', '5773.0', '5817.0', '5764.0', '5807.0', '5755.0', '5798.0', '5745.0', '5789.0', '5736.0', '5780.0', '5727.0', '5771.0']
23
['5736.0', '5789.0', '5745.0', '5798.0', '5755.0', '5807.0', '5764.0', '5817.0', '5773.0', '5729.0', '5782.0', '5738.0', '5791.0', '5748.0', '5801.0', '5757.0', '5810.0', '5766.0', '5819.0', '5775.0', '5732.0',
'5784.0', '5741.0', '5794.0', '5750.0', '5803.0', '5759.0', '5812.0', '5768.0', '5821.0', '5778.0', '5734.0', '5787.0', '5743.0', '5796.0', '5752.0', '5805.0', '5761.0', '5814.0', '5771.0', '5727.0', '5780.0']
25
['5745.0', '5803.0', '5764.0', '5821.0', '5782.0', '5743.0', '5801.0', '5761.0', '5819.0', '5780.0', '5741.0', '5798.0', '5759.0', '5817.0', '5778.0', '5738.0', '5796.0', '5757.0', '5814.0', '5775.0', '5736.0',
'5794.0', '5755.0', '5812.0', '5773.0', '5734.0', '5791.0', '5752.0', '5810.0', '5771.0', '5732.0', '5789.0', '5750.0', '5807.0', '5768.0', '5729.0', '5787.0', '5748.0', '5805.0', '5766.0', '5727.0', '5784.0']
```


Wireless communication system architecture

- RC Initialization -> NXP LPC1549
- RC initialization baseband of SPI register
- RC initialization Transceiver of SPI register
- RC Fixed frequency hopping radio
- Air Initialization -> STM32F103
- Air initialization baseband of SPI register
- Air initialization Transceiver of SPI Register
- Air Pick a high signal to noise ratio of the frequency monitor
- Air Roger that RC Synchronization signals and hopping sequence

- Write 5 Byte to the pairing code baseband

SPI address

3 , 4 , 5 , 6 , 7

- Write 5 Byte passkey

```

00007100 04 29 05 47 FF FF CB D3 01 E1 07 04 0E 15 02 2C .).G.....,
00007110 47 03 11 07 30 43 4B 4A 32 30 31 44 47 55 FF FF G...0CKJ201DGU..
00007120 FF FF FF FF 8B 6D 05 95 36 F1 2E 62 E1 9B 7E A8 .....m..6.....~
00007130 1B 6A CA FC 81 61 18 75 48 B6 21 B9 98 0B 6C B4 ...j...a.uK.!...l.
00007140 C2 45 AE 19 7E F6 A8 1D 76 D3 CB 7D 66 16 43 D7 ...~.....}f.C.
00007150 62 80 DF 86 01 23 64 1B 8E BF 01 EB EE 59 03 36 b..#d.....6
00007160 08 E0 0C 1E 00 3C 00 00 DA 02 F5 07 1C 0D 1E 00 .....<.....
00007170 3C 00 00 49 03 50 08 0E 0D 1E 00 3C 00 01 3C 03 <..I.P.....<..
00007180 3A 08 00 0D 1E 00 3C 00 01 6D 00 CB 07 55 0F C8 :....<..m...U..
00007190 00 C8 00 00 02 FF FF FF FF 0A 49 8A 59 0C 0B 13 .....I.Y...
000071A0 07 00 0A 00 06 06 06 06 06 06 06 06 06 06 06 .....
000071B0 06 06 06 06 06 06 06 06 06 06 06 06 06 06 06 .....
000071C0 06 06 06 06 06 06 06 06 06 06 06 06 06 06 06 .....
000071D0 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
000071E0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
000071F0 00 00 00 00 00 00 00 00 A3 A3 A3 A2 A2 A2 A1 .....
00007200 A1 A1 A1 A0 A0 A0 A0 9F 9F 9F 9E 9E 9D 9D 9C .....
00007210 .....
0001CCA0 .....
0001CCA0 spi02bb_paircode .....
0001CCA0 PUSH {R4,LR} .....
0001CCA2 MOV R4, R0 .....
0001CCA4 MOVS R0, #1 .....
0001CCA6 BL spi_read .....
0001CCAA LDRB R1, [R4] .....
0001CCAC MOVS R0, #3 .....
0001CCAE BL spi_write1byte .....
0001CCB2 LDRB R1, [R4,#1] .....
0001CCB4 MOVS R0, #4 .....
0001CCB6 BL spi_write1byte .....
0001CCBA LDRB R1, [R4,#2] .....
0001CCBC MOVS R0, #5 .....
0001CCBE BL spi_write1byte .....
0001CCC2 LDRB R1, [R4,#3] .....
0001CCC4 MOVS R0, #6 .....
0001CCC6 BL spi_write1byte .....
0001CCCA LDRB R1, [R4,#4] .....
0001CCCC MOVS R0, #7 .....
0001CCCE BL spi_write1byte .....
0001CCD2 POP.W {R4,LR} .....
0001CCD6 MOVS R0, #2 .....
0001CCD8 B.W spi_read .....
0001CCD8 ; End of function spi02bb_paircode

```


Wireless communication system architecture

- RC versus Air Synchronization principle
- RC Hopping cycle is set

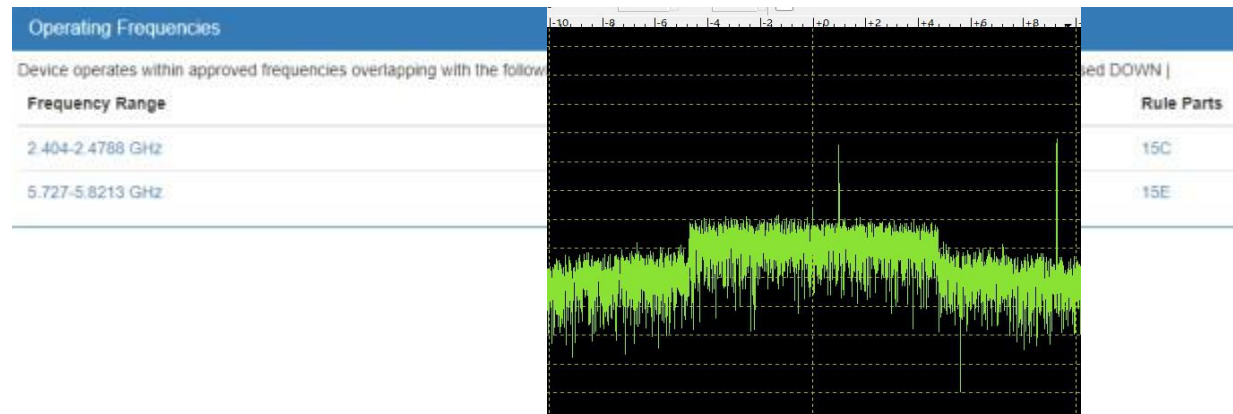
```
rx freq 5845
rx freq 5825
tx freq 5738
rx freq 5845
rx freq 5830
tx freq 5782
rx freq 5845
rx freq 5835
```

rx Hopping setting ---- 0.3ms --- tx Hopping setting ---- 3.075ms ---- rx Figure pass setting ---- 13.69ms --- rx Set the next frequency hopping

- Air Hopping cycle is set

rx Image transmission settings ---- 0.3ms --- rx Hopping setting ---- 2.91ms ---- tx Image transmission data transmission setting ---- 10.78ms --- rx Image transmission settings

```
rx freq 5845
rx freq 5738
tx freq 5845
rx freq 5845
rx freq 5782
tx freq 5845
rx freq 5845
```



2.400 - 2.483 GHz和5.725 - 5.825 GHz

2.400 - 2.483 GHz (无干扰、无遮挡)

FCC : 7000 m

CE : 3500 m

SRRC : 4000 m

5.725 - 5.825 GHz (无干扰、无遮挡)

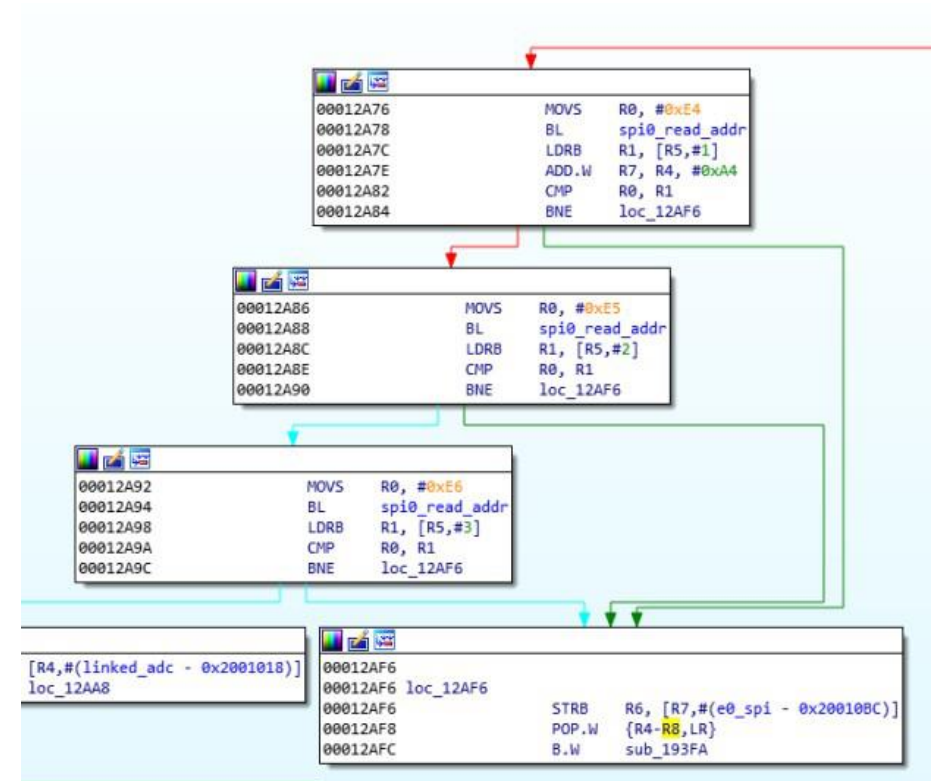
FCC : 7000 m

CE : 2000 m

SRRC : 5000 m

Wireless communication system architecture

- RC verification Air pair
- RC Read baseband SPI address(0xe4,0xe5,0xe6) Values are compared



How to hijack a UAV

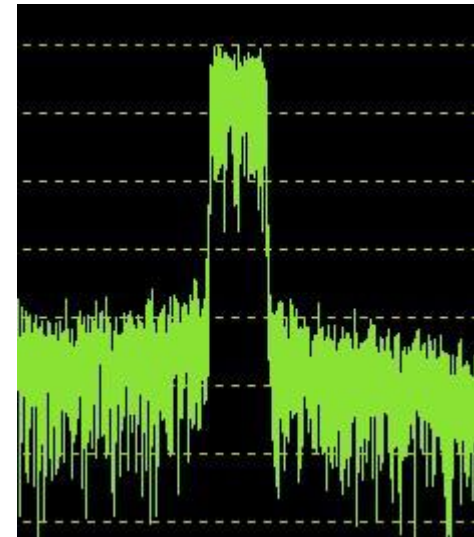
- By pairing crack the code, the code word space 0x1000000
- Reform RC Firmware, fixed frequency intervals 10ms initialization baseband SPI Pairing code register
- At intervals of 10ms by SDR Fixed frequency reproduction Air signal
- Read baseband SPI register(0xe4,0xe5,0xe6) Values are compared
- The result is written to the serial port
- Crack need offline operation, not in real time
- Theoretically break up just a conservative estimate 46 hour
- Successful break can remotely modify the aircraft pairing code and take complete control of UAV

Todo list:

Successfully injected code into RC Firmware, crack the

algorithm by writing test code constructs RC Firmware

verification test



Anti-drone technology transfer confrontation

- Stm32 IO remap defeat SWD debugging
- Peripheral hardware detection, ADC Particle Size Determination
- Atmel chip Security Bit
- Switch protection circuit against SWD reset signal

```
SUB      SP, SP, #0x20
BL      sub_800D7B8
MOVS     R1, #1
MOV      R0, R1
BL      RCC_APB2PeriphClockCmd
MOVS     R1, #1
LDR      R0, =0x300400 ; Full SWJ Disabled (JTAG-DP + SW-DP)
BL      GPIO_PinRemapConfig
ADD      R0, SP, #0x20+var_14
```

```
00BE14 set_jreset_io_disable ; CODE XREF: sub_800D588+524p
00BE14
00BE14 var_8 = -8
00BE14 var_6 = -6
00BE14 var_5 = -5
```

```
PUSH     {R3,LR}
MOVS     R1, #1
MOVS     R0, #4
BL      RCC_APB2PeriphClockCmd
MOV.W    R0, #0x8000
STRH.W   R0, [SP,#8+var_8]
MOVS     R0, #3
STRB.W   R0, [SP,#8+var_6]
MOVS     R0, #4
STRB.W   R0, [SP,#8+var_5]
MOV      R1, SP
LDR      R0, =0x40010800
BL      GPIO_Init ; PA15 disable JTDI
POP
```

```
PUSH     {R3,LR}
MOVS     R1, #1
MOVS     R0, #8
BL      RCC_APB2PeriphClockCmd
MOVS     R0, #0x10
STRH.W   R0, [SP,#8+var_8]
MOVS     R1, #3
STRB.W   R1, [SP,#8+var_6]
STRB.W   R0, [SP,#8+var_5]
LDR      R0, =0x40010C0C
MOV      R1, SP
SUBS     R0, #0xC
BL      GPIO_Init ; PB4
```


follow up research

- OTA Upgrade to crack agreement
- Constructed some hardware modules and firmware upgrade (Smart Battery, LightBridge)
- Fuzzing Flight control protocol interface
- SDR Analog wireless communication

Q & A



Thanks
vessialq@gmail.com