The Birdman
and Cospas-Sarsat Satellites

WHO WE ARE

360 TECHNOLOGY

Security Research Institute

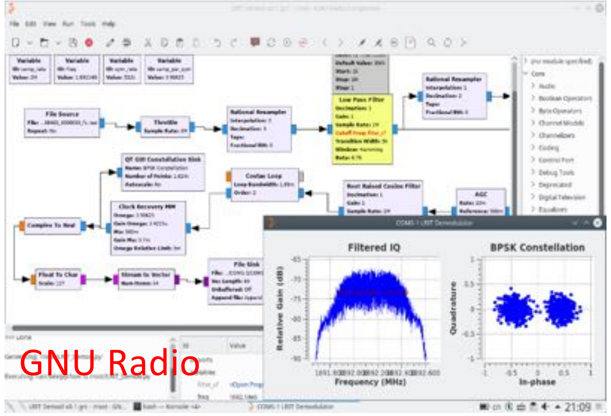
Unicorn Team

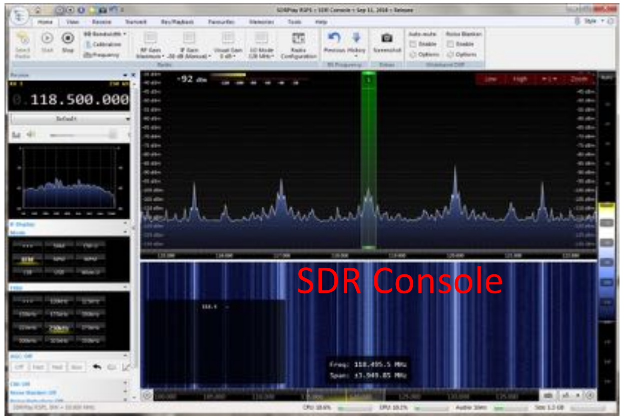
360
www.360.cn

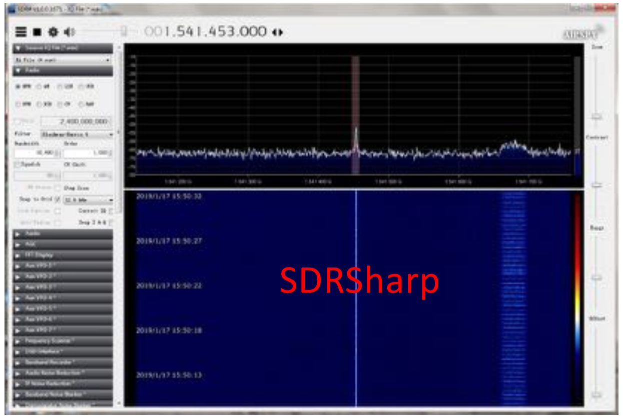
SECURITY RESEARCH INSTITUTE
HARDWARE - RADIO 360

001.692.140.000
AMATEUR

Common Tools



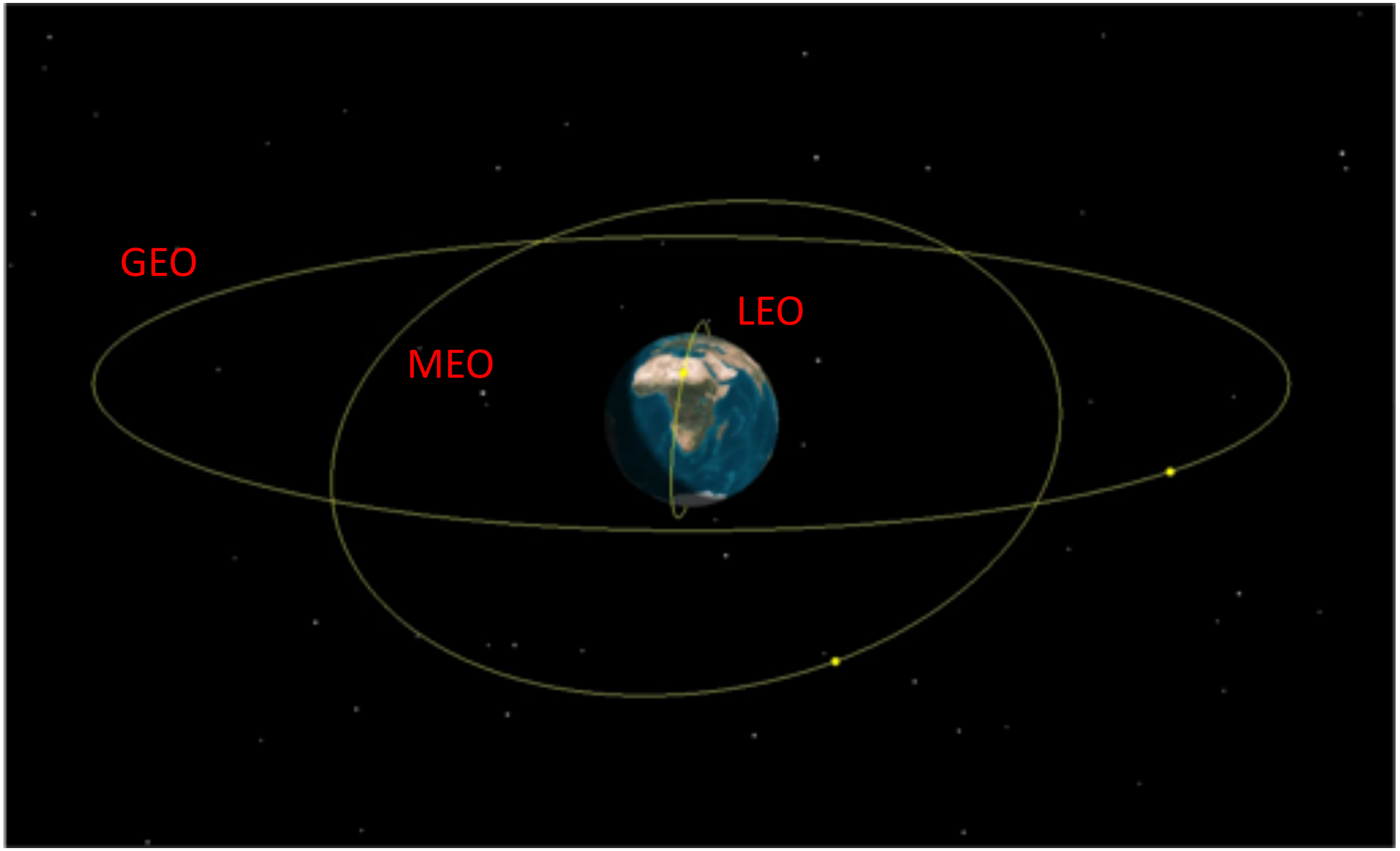


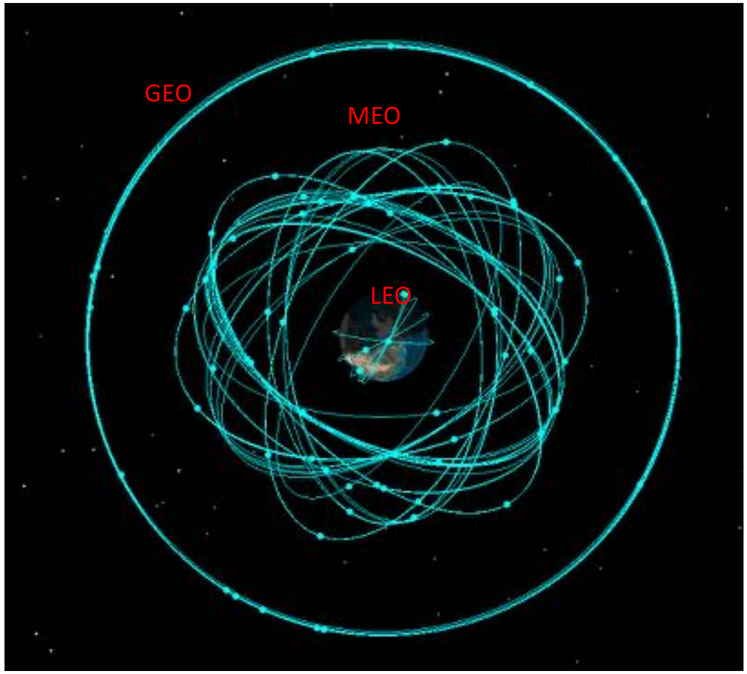


Satellite orbit

Satellite TLE data by NORAD
(North American Aerospace Defense Command)

SGP4 SDP4 SGP8 SDP8





How to catch LEO orbit satellite?

For tracking those flying satellites we need an auto-tracking antenna.

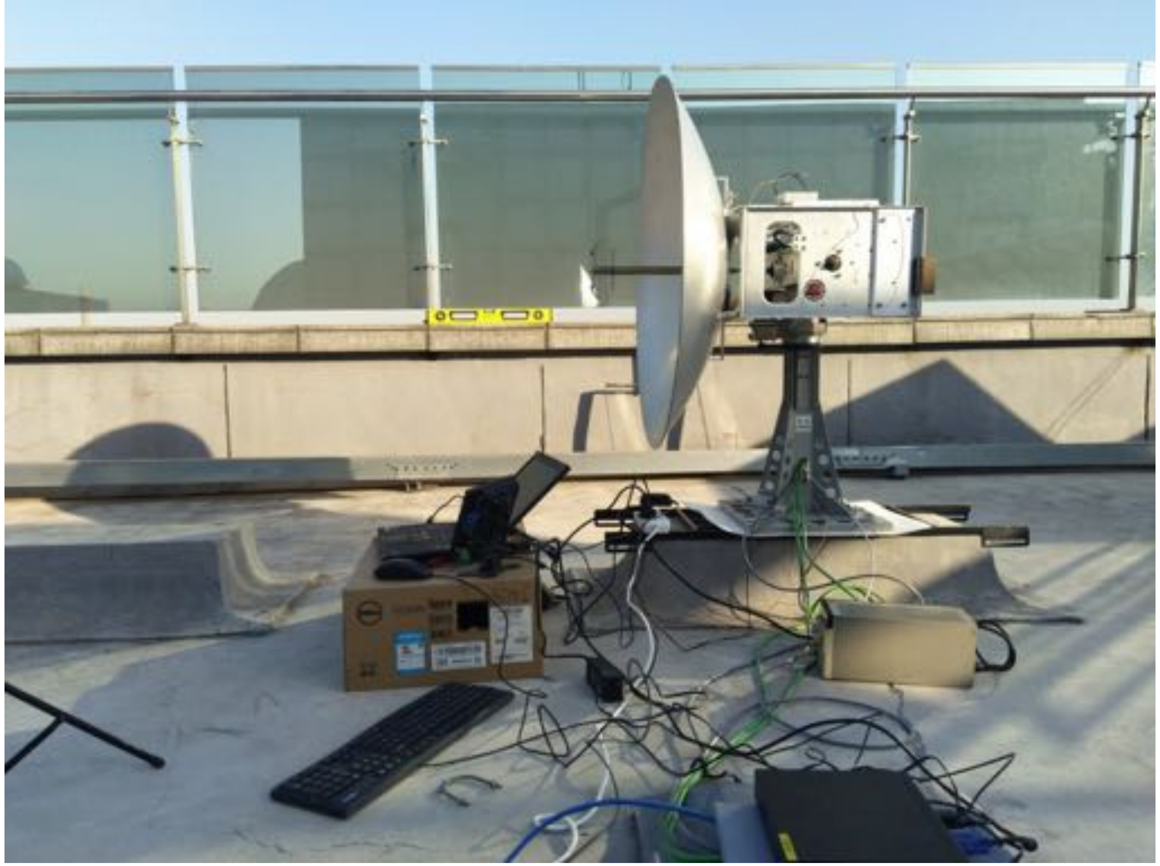
OpenATS made by myself.

L-band Gain ： 15~16dBi

LNA Gain ： 50dB

LNA Noise Factor: 0.7dB

Antenna Diameter: 0.9m



OpenATS https://github.com/openats/openats

Found something unusual ！

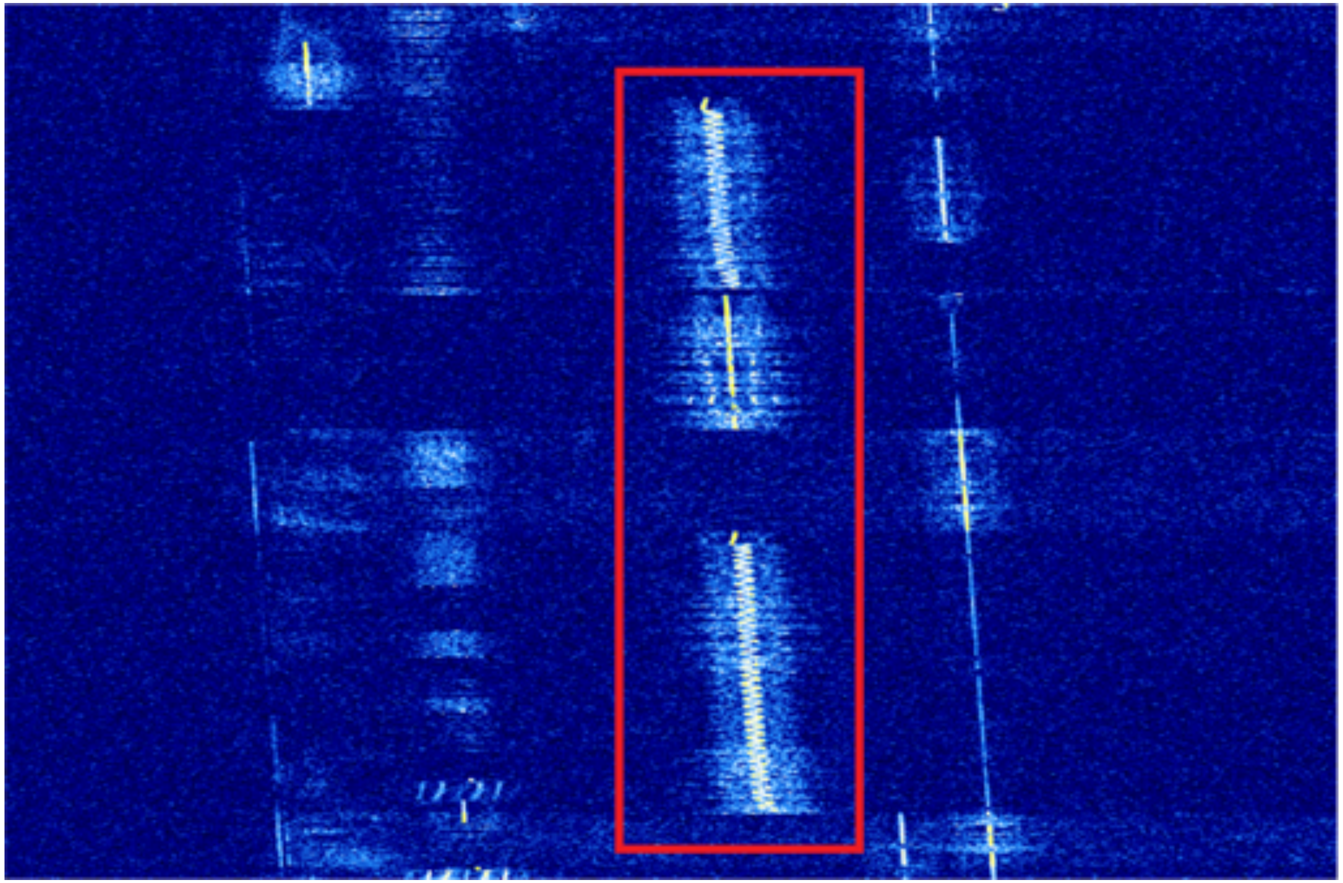
Found something unusual !

It’s looks like an analog signal with the doppler shift.

The signal’s center frequency is 1544.5MHz

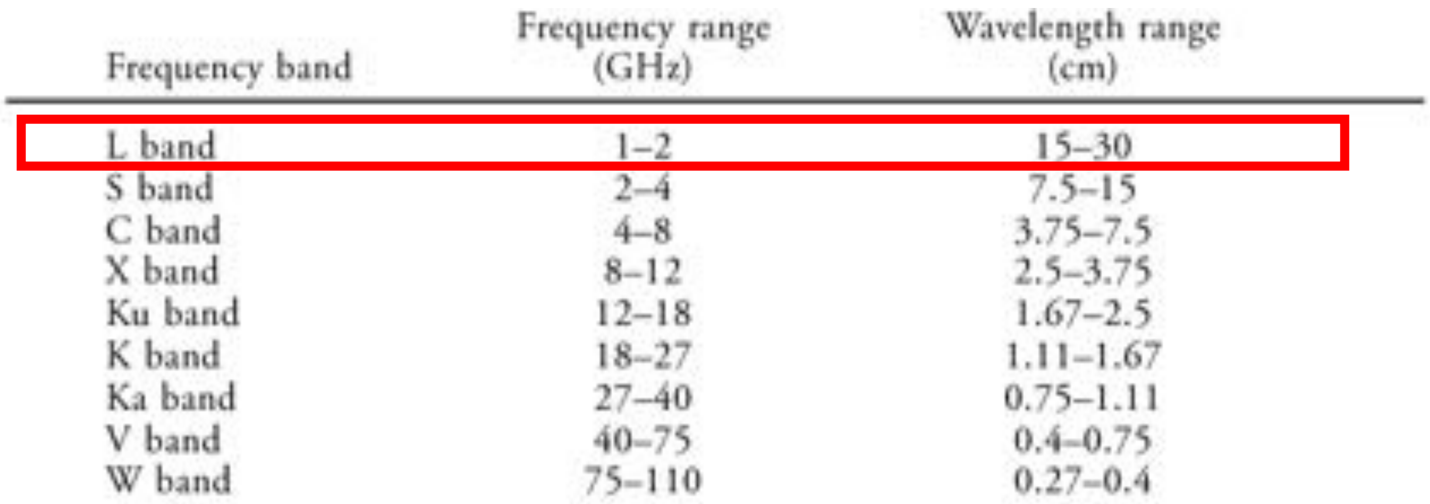
Wow!

I can hear someone is speaking !!!



L-band
1544.5MHz?

L-Band

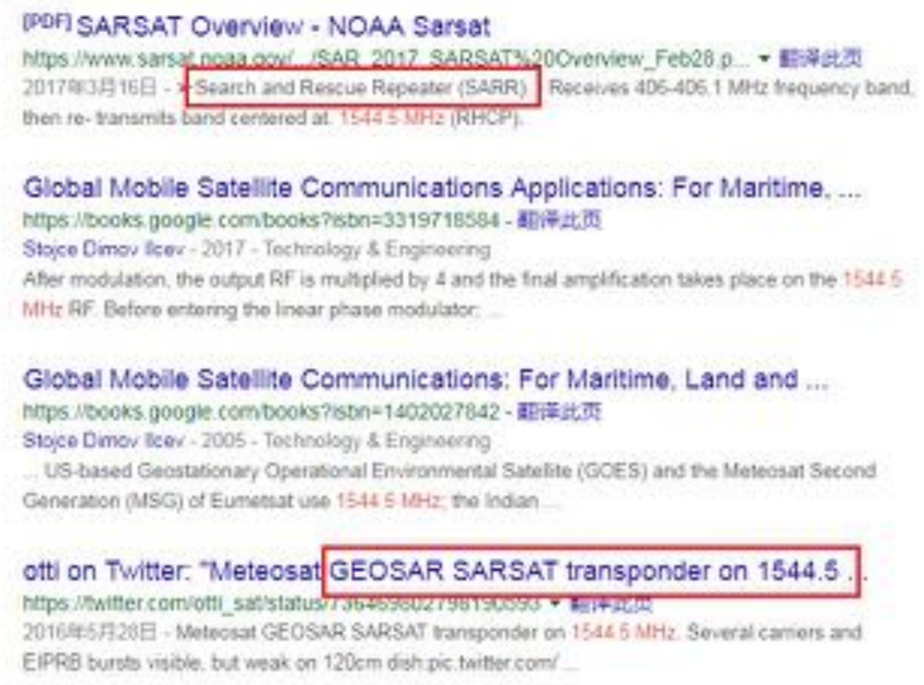


Frequency band	Frequency range (GHz)	Wavelength range (cm)
L band	1–2	15–30
S band	2–4	7.5–15
C band	4–8	3.75–7.5
X band	8–12	2.5–3.75
Ku band	12–18	1.67–2.5
K band	18–27	1.11–1.67
Ka band	27–40	0.75–1.11
V band	40–75	0.4–0.75
W band	75–110	0.27–0.4

- Frequency range : 1GHz – 2GHz
- Mainly used for aviation and marine communications, access to terrestrial information via satellite.
- Be classified as *meteorological satellites*, *navigation satellites*, and *communication satellites*.

1544.5MHz

It’s a system called
COSPAS-SARSAT,
which downlink frequency
is 1544.5MHz,
from NOAA-18 satellite.

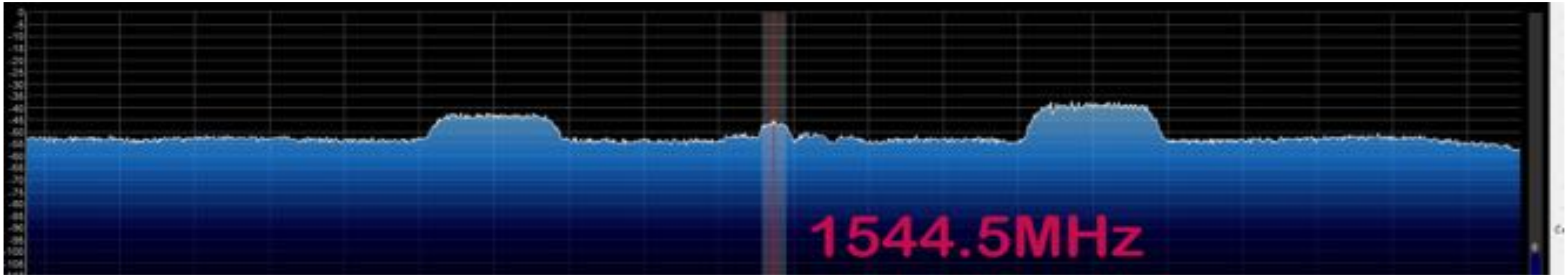


[PDF] SARSAT Overview - NOAA Sarsat
https://www.sarsat.noaa.gov/.../SAR_2017_SARSAT%20Overview_Feb28.p... ▾ 翻译此页
2017年3月16日 - • Search and Rescue Repeater (SARR). Receives 406-406.1 MHz frequency band, then re- transmits band centered at 1544.5 MHz (RHCP).

Global Mobile Satellite Communications Applications: For Maritime, ...
https://books.google.com/books?isbn=3319718584 - 翻译此页
Stojce Dimov Ilcev - 2017 - Technology & Engineering
After modulation, the output RF is multiplied by 4 and the final amplification takes place on the 1544.5 MHz RF. Before entering the linear phase modulator: ...

Global Mobile Satellite Communications: For Maritime, Land and ...
https://books.google.com/books?isbn=1402027842 - 翻译此页
Stojce Dimov Ilcev - 2005 - Technology & Engineering
... US-based Geostationary Operational Environmental Satellite (GOES) and the Meteosat Second Generation (MSG) of Eumetsat use 1544.5 MHz; the Indian ...

otti on Twitter: "Meteosat GEOSAR SARSAT transponder on 1544.5 ...
https://twitter.com/otti_sat/status/736459602798190593 ▾ 翻译此页
2016年5月28日 - Meteosat GEOSAR SARSAT transponder on 1544.5 MHz. Several carriers and EIPRB bursts visible, but weak on 120cm dish pic.twitter.com/ ...



What’s the COSPAS-SARSAT ?

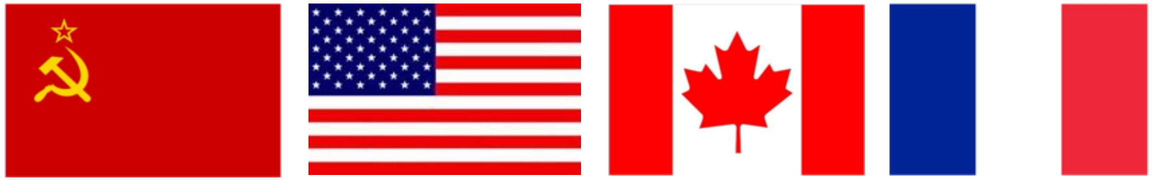
COSPAS-SARSAT

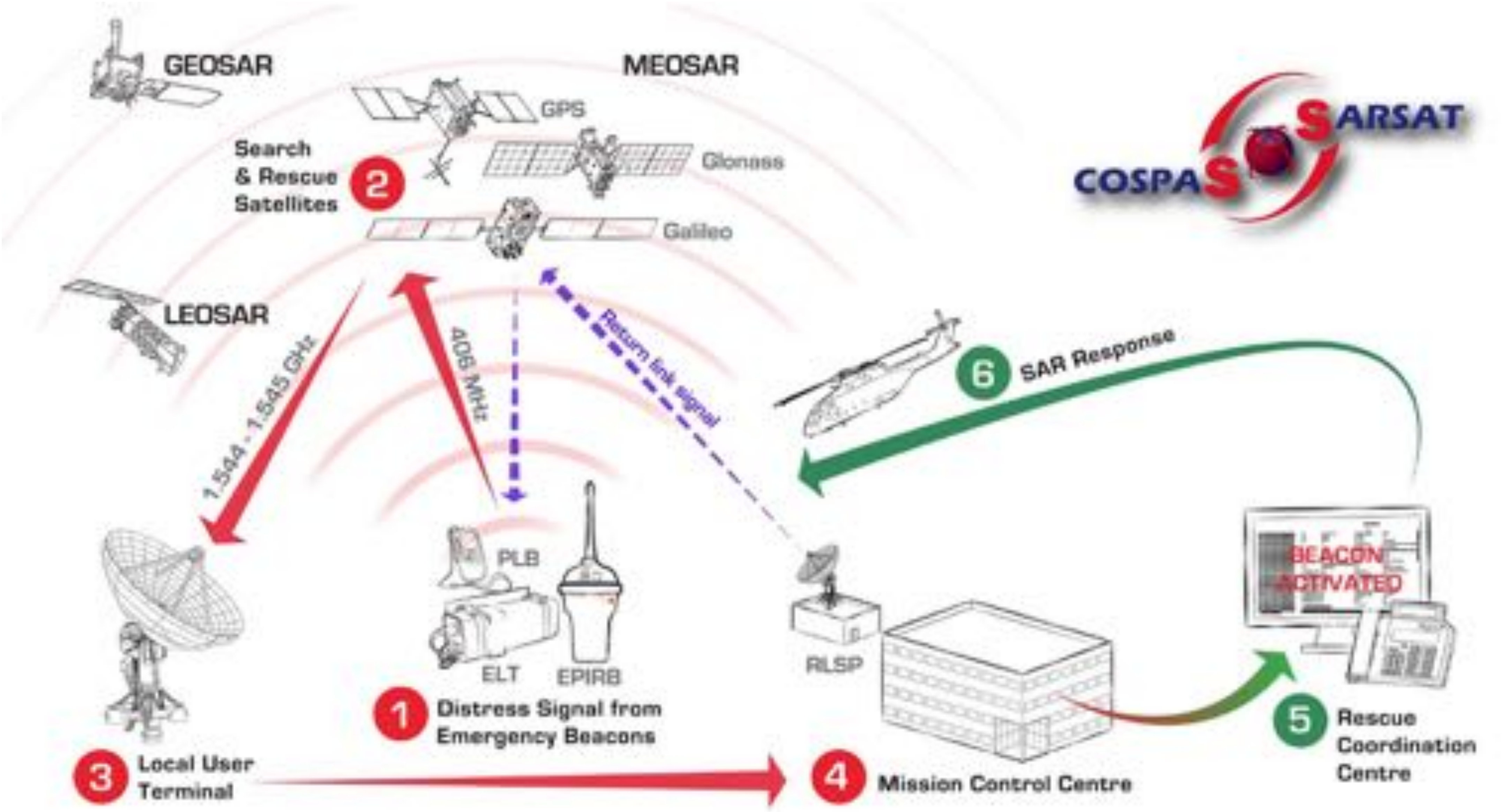
Search And Rescue Satellites-Aided Tracking System

The first satellite “COSPAS-1” launched in 1982.

The four original member nations:

Soviet Union, United States, Canada and France




GEOSAR
MEOSAR
GPS
Glonass
Galileo
Search & Rescue Satellites
2
LEOSAR
COSPAS SARSAT
1.544 - 1.545 GHz
406 MHz
Return link signal
6
SAR Response
PLB
ELT
EPIRB
RLSP
BEACON ACTIVATED
1
Distress Signal from Emergency Beacons
3
Local User Terminal
4
Mission Control Centre
5
Rescue Coordination Centre

Emergency Beacons

Beacons can be activated either manually or automatically when you are in danger. The beacons also can transmit a GPS position within a distress alert.

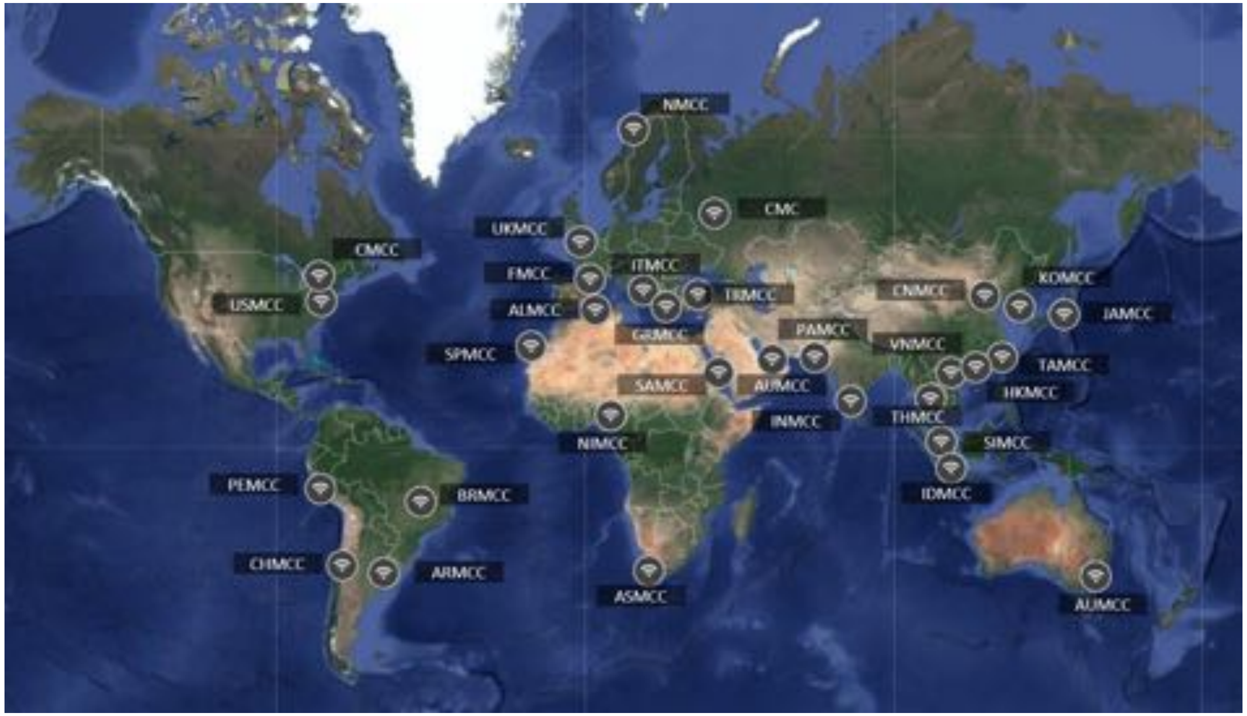
ELT Aviation

PLB Personal portable

EPIRB Maritime

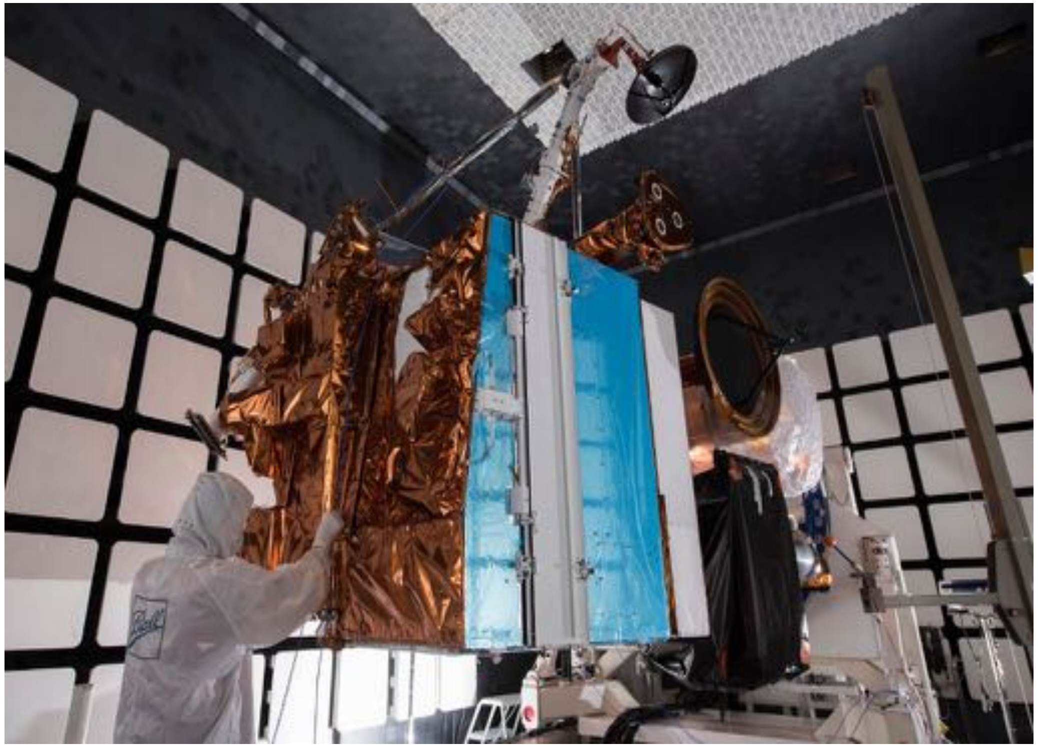
Ground Stations

User states and organizations that operate 94 LUTs(local user terminal) station and 34+ MCCs(mission control centers) worldwide.



Satellites

Metop-C



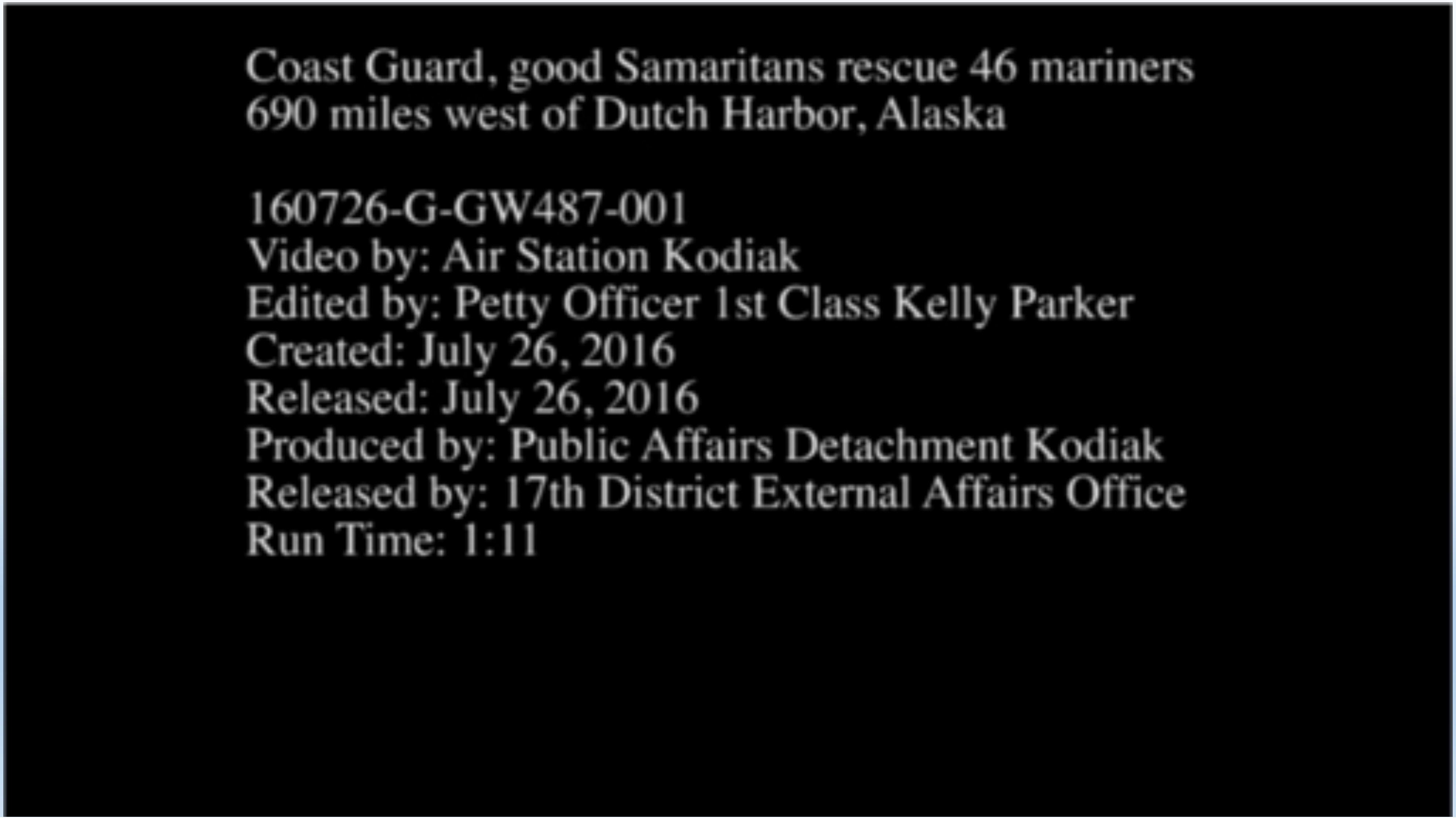
JPSS-1(NOAA-20)

A Great System

Since the inception of the system in 1982, more than 41,000 rescues have been supported and over 35,000 lives have been rescued worldwide.

That's a great system !

Rescue video provide by NOAA



Coast Guard, good Samaritans rescue 46 mariners
690 miles west of Dutch Harbor, Alaska

160726-G-GW487-001
Video by: Air Station Kodiak
Edited by: Petty Officer 1st Class Kelly Parker
Created: July 26, 2016
Released: July 26, 2016
Produced by: Public Affairs Detachment Kodiak
Released by: 17th District External Affairs Office
Run Time: 1:11

What is the content of the distress signal?

0x01

Find the protocol for the SARSAT system from official documents

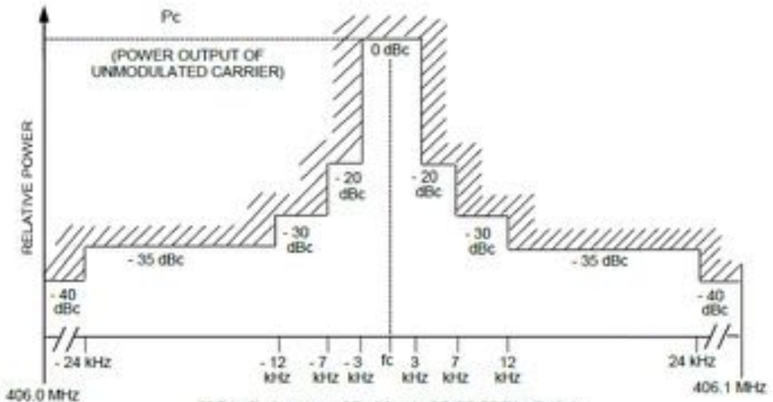
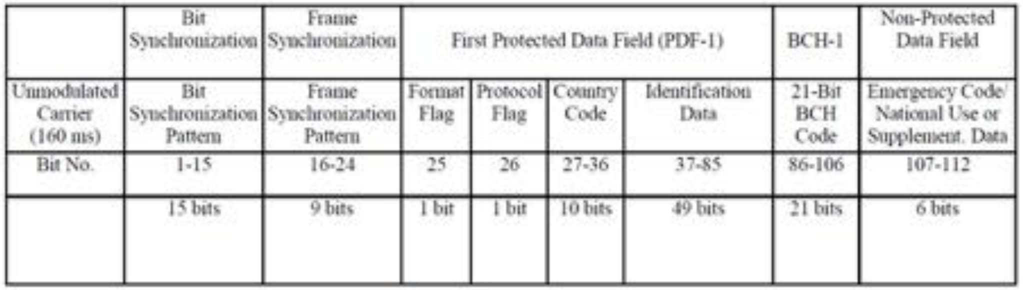


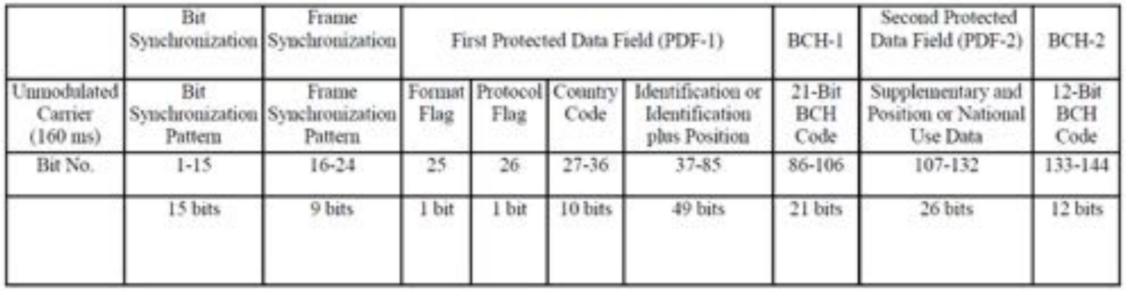
Figure 2.3: Spurious Emission Mask for 406.0 to 406.1 MHz Band

Figure A1: Data Fields of the Short Message Format



	Bit Synchronization	Frame Synchronization	First Protected Data Field (PDF-1)				BCH-1	Non-Protected Data Field
Unmodulated Carrier (160 ms)	Bit Synchronization Pattern	Frame Synchronization Pattern	Format Flag	Protocol Flag	Country Code	Identification Data	21-Bit BCH Code	Emergency Code/ National Use or Supplement. Data
Bit No.	1-15	16-24	25	26	27-36	37-85	86-106	107-112
	15 bits	9 bits	1 bit	1 bit	10 bits	49 bits	21 bits	6 bits

Figure A2: Data Fields of the Long Message Format



	Bit Synchronization	Frame Synchronization	First Protected Data Field (PDF-1)				BCH-1	Second Protected Data Field (PDF-2)	BCH-2
Unmodulated Carrier (160 ms)	Bit Synchronization Pattern	Frame Synchronization Pattern	Format Flag	Protocol Flag	Country Code	Identification or Identification plus Position	21-Bit BCH Code	Supplementary and Position or National Use Data	12-Bit BCH Code
Bit No.	1-15	16-24	25	26	27-36	37-85	86-106	107-132	133-144
	15 bits	9 bits	1 bit	1 bit	10 bits	49 bits	21 bits	26 bits	12 bits

https://cospas-sarsat.int/en/beacon-regulations-handbook

0x02

Get important informations of this system.

- Modulation : BPSK
- Sambol Rate : 400bps
- 3dB Bandwidth :
  406.025MHz/406.050MHz(80KHz)
- Uplink power : 35~39dBm/3W~8W
- Uplink Freq：
  406MHz (406.025MHz,406.050MHz…)
- Downlink Freq :
  1544.5MHz (NOAA,GOES,GPS,METOP)
  1541.45MHz (Inmarsat)
  1544.1MHz (Galileo)
  1544.9MHz (Glonass)
  2226.47234MHz (GPS-Ⅲ、DASS)
  4503.385MHz/4504.2MHz/4507.0MHz (INSAT)

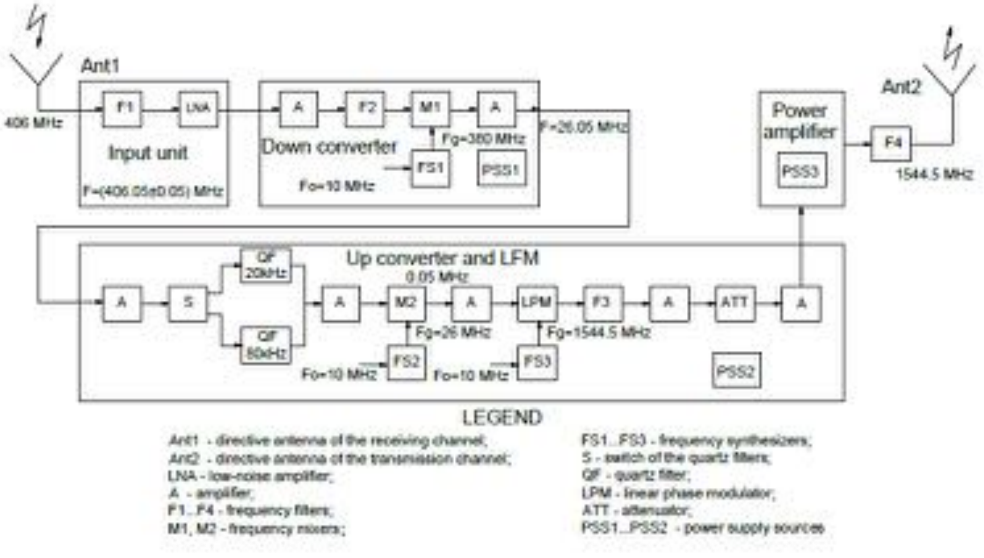

Ant1
406 MHz
F1
LNA
Input unit
F=(406.05±0.05) MHz
A
F2
M1
A
Down converter
Fg=380 MHz
FS1
PSS1
Fo=10 MHz
F=26.05 MHz
Power amplifier
PSS3
Ant2
F4
1544.5 MHz
Up converter and LFM
QF 20kHz
QF 80kHz
A
S
0.05 MHz
M2
LPM
F3
ATT
Fg=26 MHz
Fg=1544.5 MHz
FS2
FS3
Fo=10 MHz
Fo=10 MHz
PSS2
LEGEND
Ant1 - directive antenna of the receiving channel;
Ant2 - directive antenna of the transmission channel;
LNA - low-noise amplifier;
A - amplifier;
F1...F4 - frequency filters;
M1, M2 - frequency mixers;
FS1...FS3 - frequency synthesizers;
S - switch of the quartz filters;
QF - quartz filter;
LPM - linear phase modulator;
ATT - attenuator;
PSS1...PSS2 - power supply sources

Figure 5.1: Electro-L SAR Functional Diagram

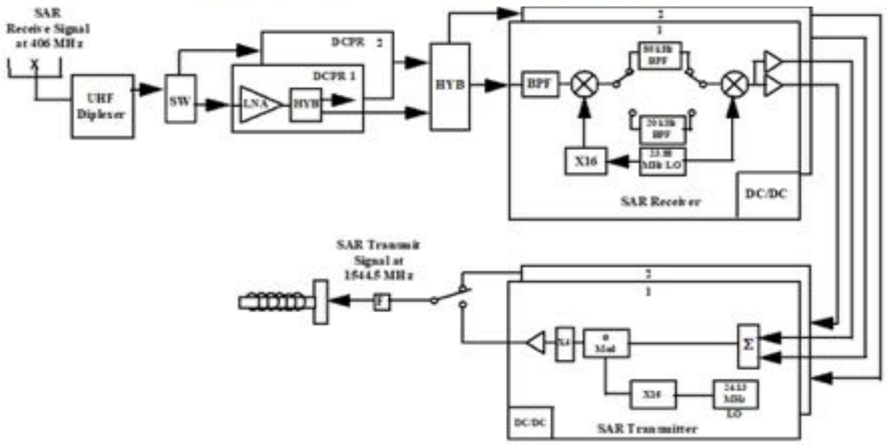


Figure 3.1: GOES-15 and before Search and Rescue Repeater Functional Diagram

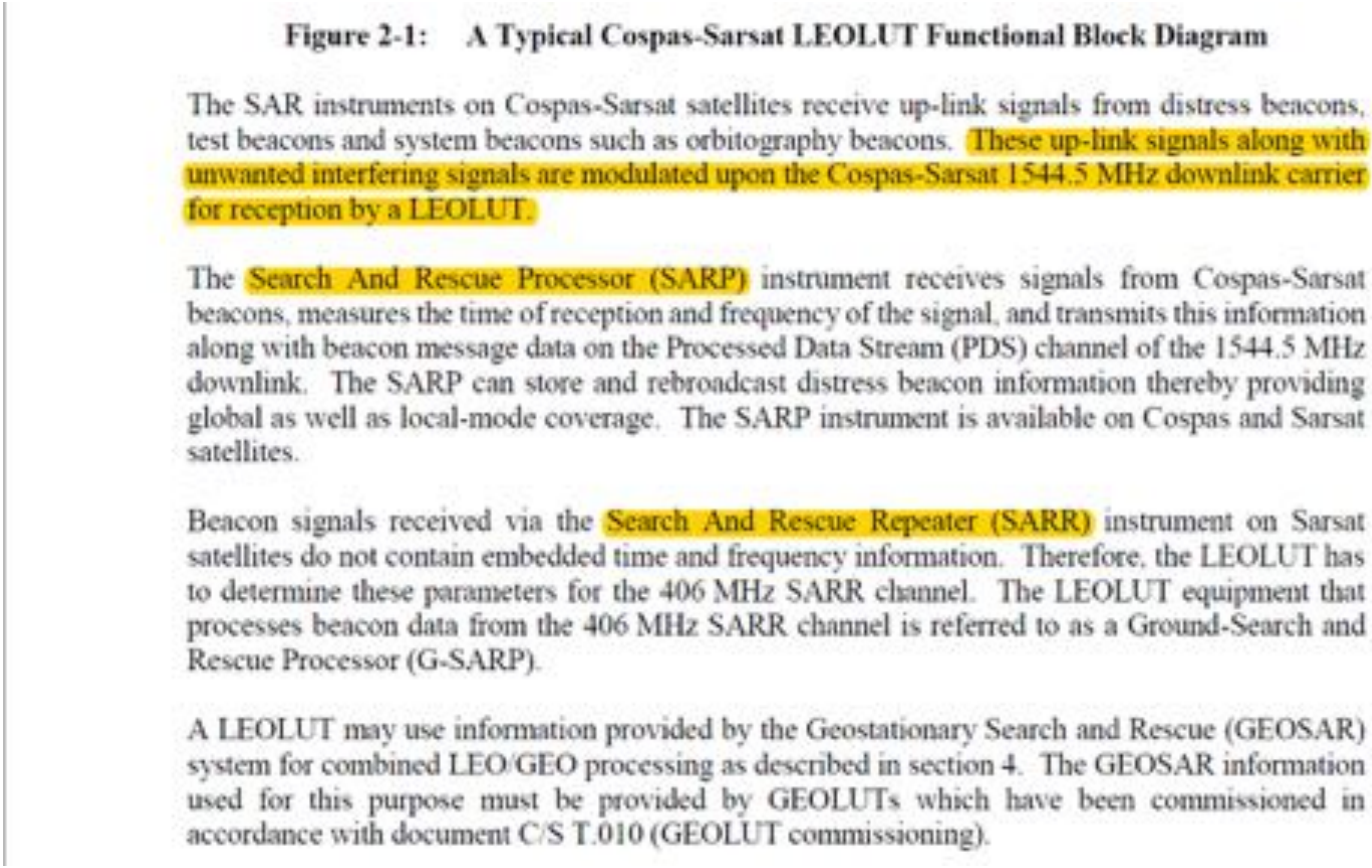


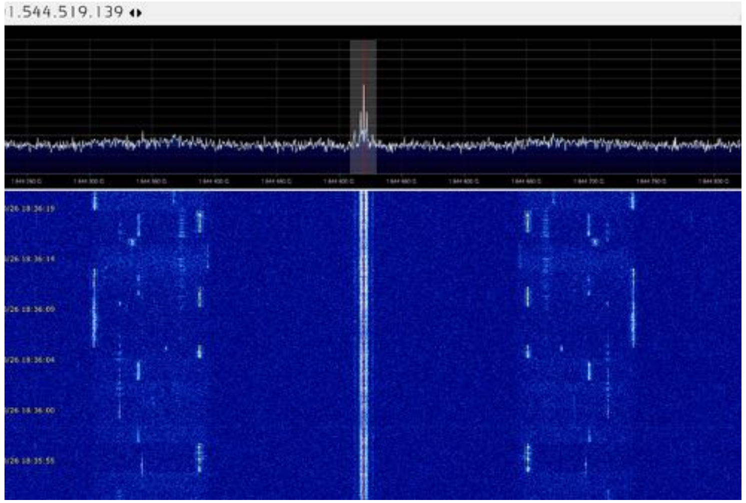
Figure 2-1: A Typical Cospas-Sarsat LEOLUT Functional Block Diagram

The SAR instruments on Cospas-Sarsat satellites receive up-link signals from distress beacons, test beacons and system beacons such as orbitography beacons. These up-link signals along with unwanted interfering signals are modulated upon the Cospas-Sarsat 1544.5 MHz downlink carrier for reception by a LEOLUT.

The Search And Rescue Processor (SARP) instrument receives signals from Cospas-Sarsat beacons, measures the time of reception and frequency of the signal, and transmits this information along with beacon message data on the Processed Data Stream (PDS) channel of the 1544.5 MHz downlink. The SARP can store and rebroadcast distress beacon information thereby providing global as well as local-mode coverage. The SARP instrument is available on Cospas and Sarsat satellites.

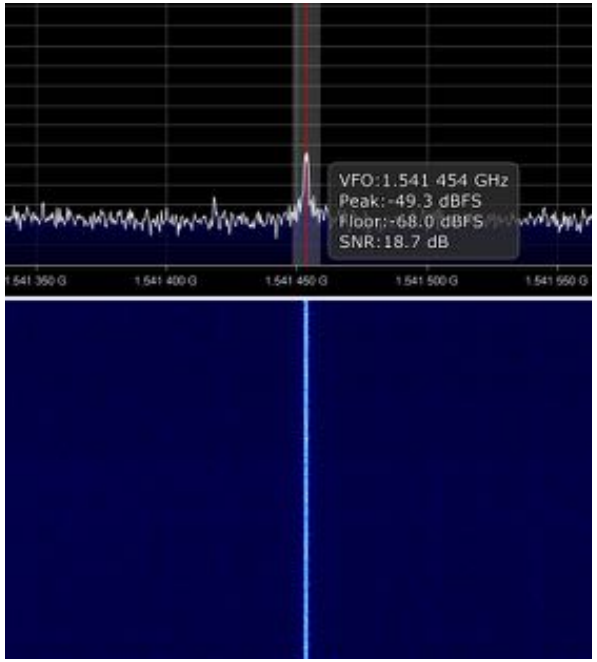
Beacon signals received via the Search And Rescue Repeater (SARR) instrument on Sarsat satellites do not contain embedded time and frequency information. Therefore, the LEOLUT has to determine these parameters for the 406 MHz SARR channel. The LEOLUT equipment that processes beacon data from the 406 MHz SARR channel is referred to as a Ground-Search and Rescue Processor (G-SARP).

A LEOLUT may use information provided by the Geostationary Search and Rescue (GEOSAR) system for combined LEO/GEO processing as described in section 4. The GEOSAR information used for this purpose must be provided by GEOLUTs which have been commissioned in accordance with document C/S T.010 (GEOLUT commissioning).



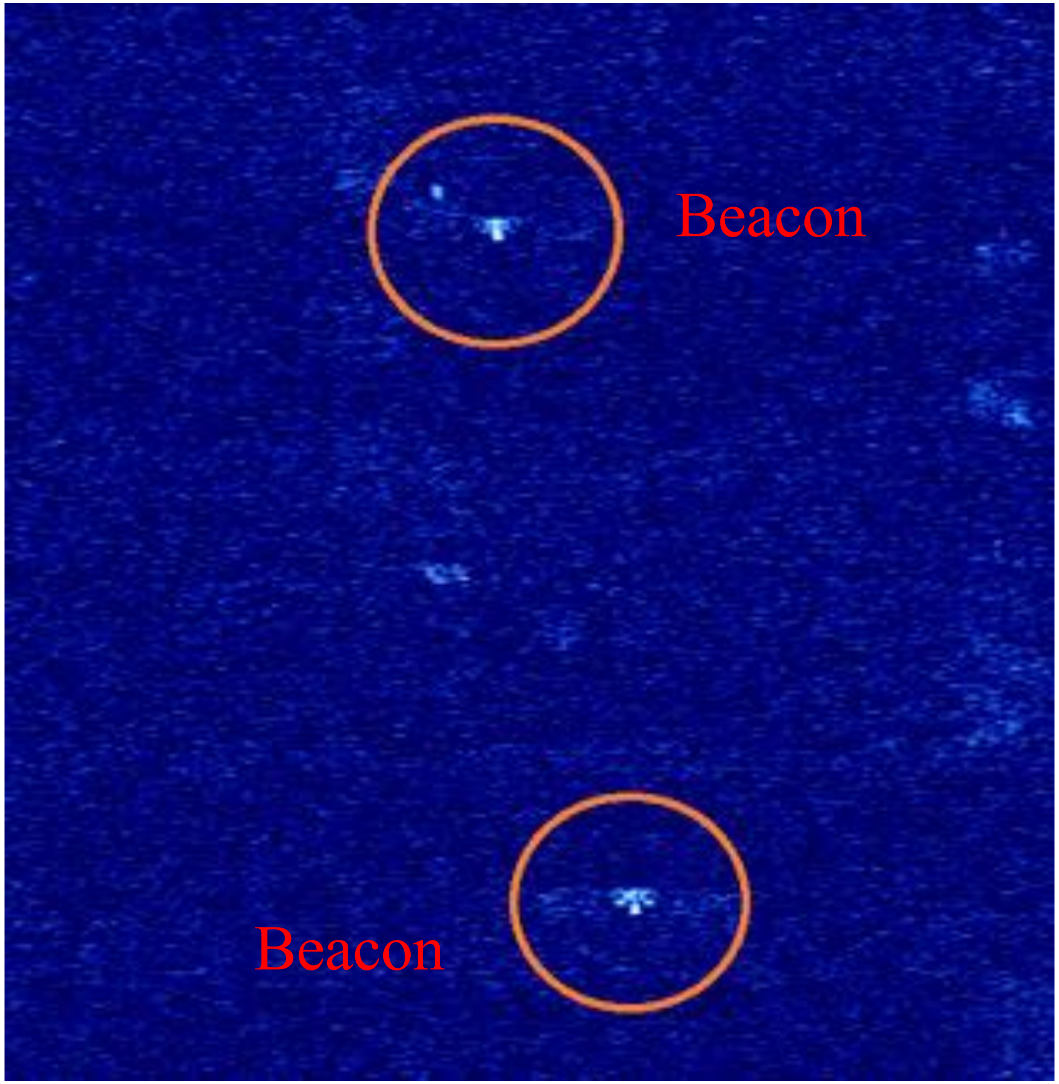
1.544.519.139

NOAA



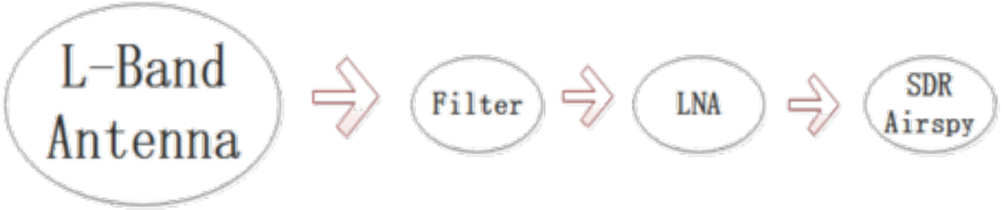
VFO:1.541 454 GHz
Peak:-49.3 dBFS
Floor:-68.0 dBFS
SNR:18.7 dB

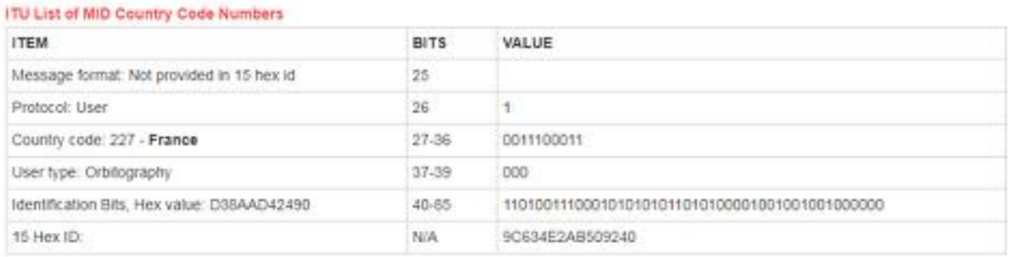
Inmarsat F3



0x03

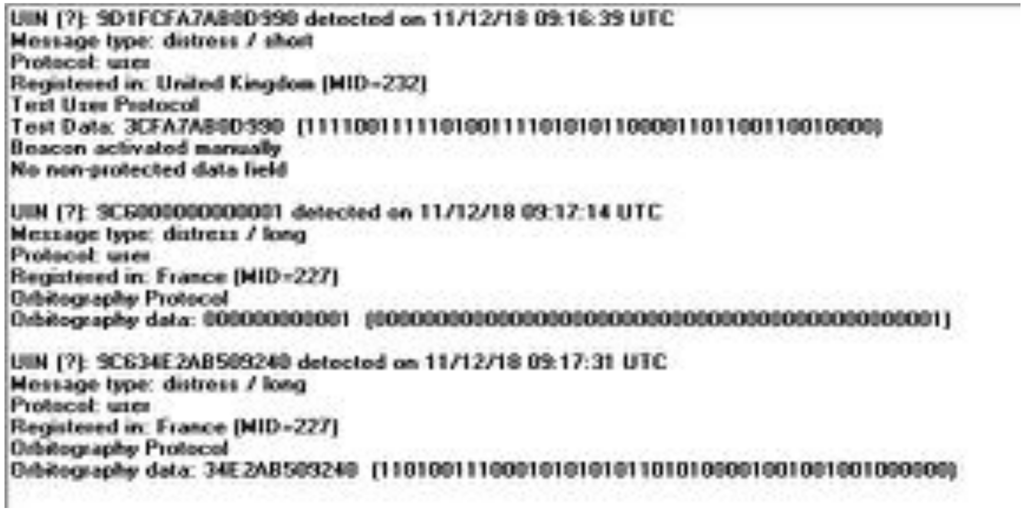
Decode the SARSAT messages through EpirbPlotter and MULTIPSK.



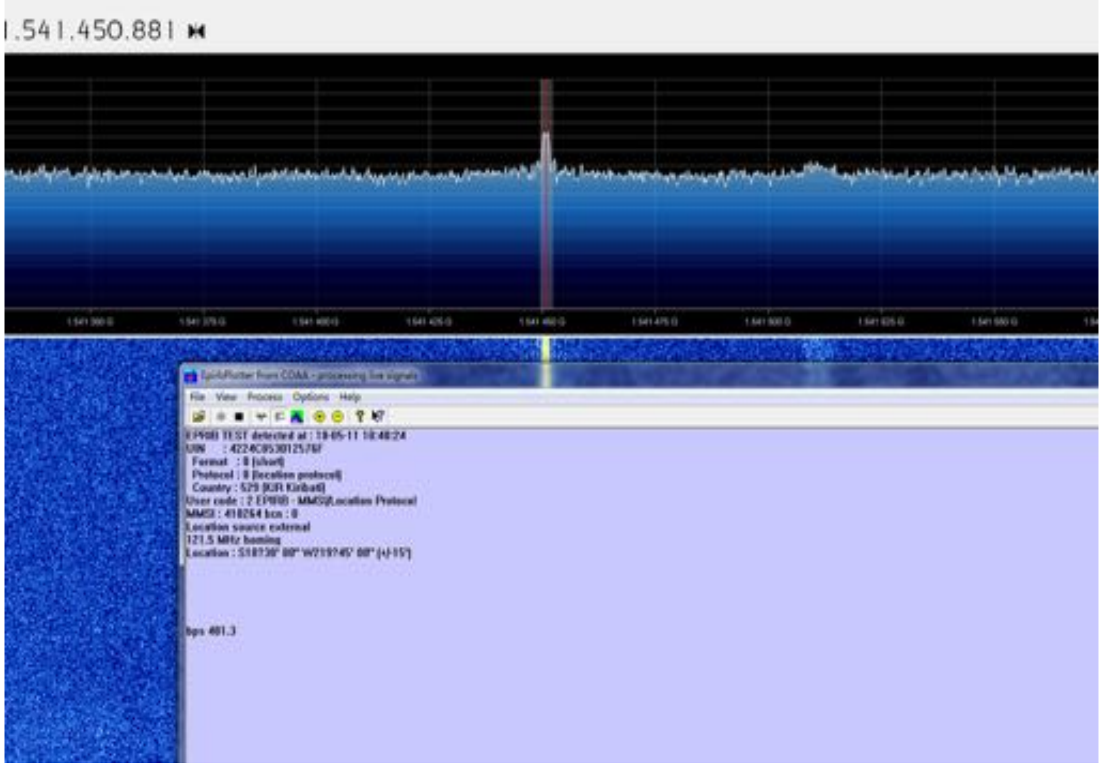


ITU List of MID Country Code Numbers

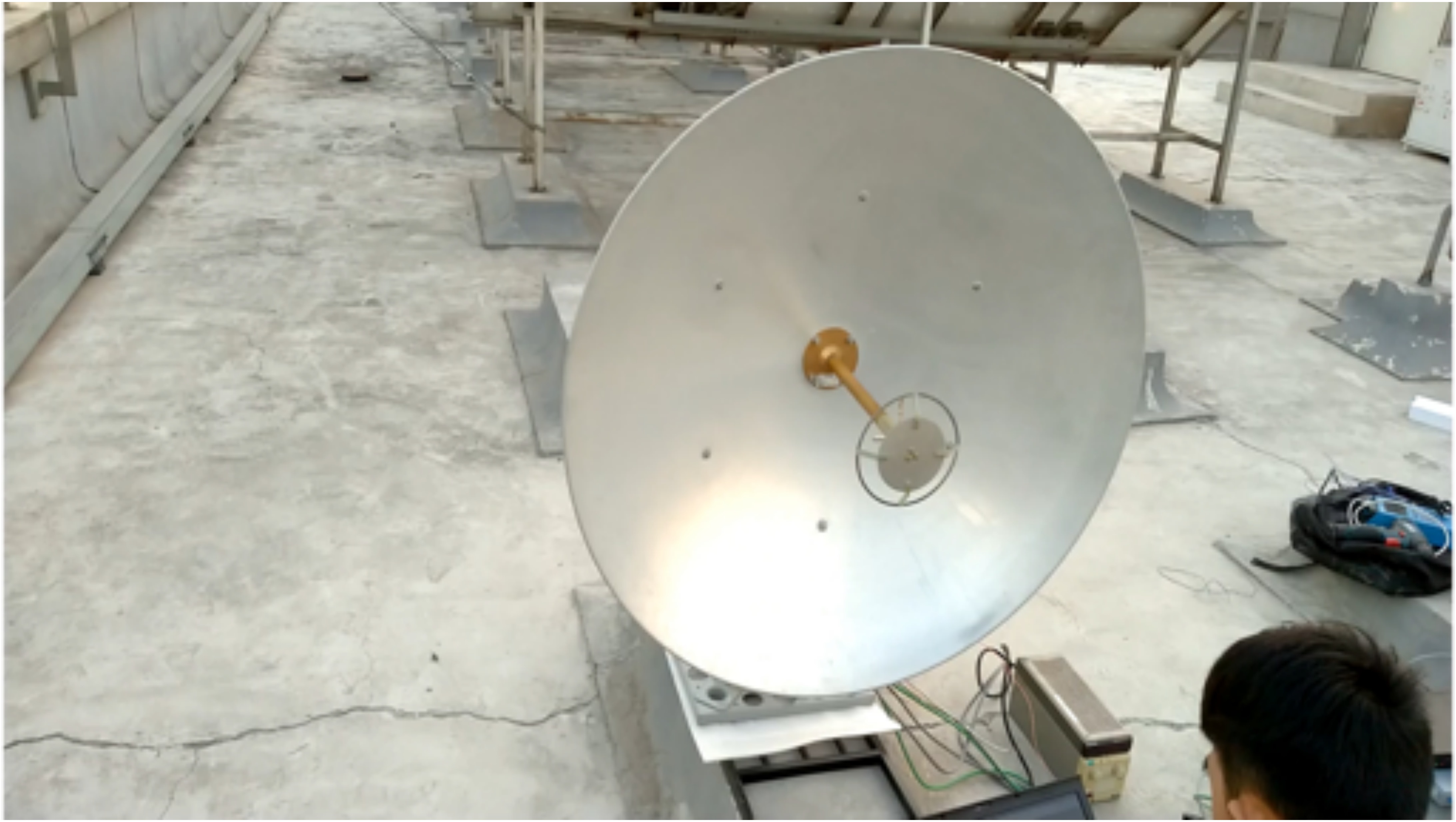
ITEM	BITS	VALUE
Message format: Not provided in 15 hex id	25	
Protocol: User	26	1
Country code: 227 - **France**	27-36	0011100011
User type: Orbitography	37-39	000
Identification Bits, Hex value: D38AAD42490	40-65	11010011100010101010110101000010010010010000000
15 Hex ID:	N/A	9C634E2AB509240

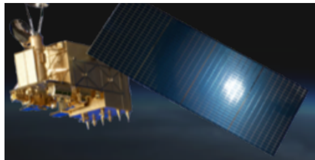


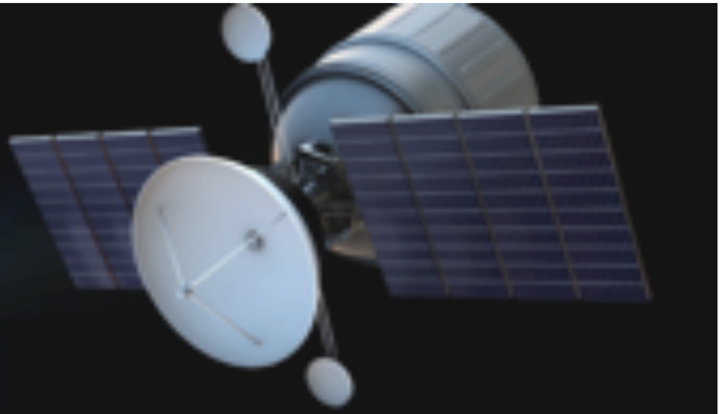
```
UIN (?): 9D1FCFA7A80D990 detected on 11/12/18 09:16:39 UTC
Message type: distress / short
Protocol: user
Registered in: United Kingdom (MID=232)
Test User Protocol
Test Data: 3CFA7A80D990  (111100111110100111101010110000110110011001000)
Beacon activated manually
No non-protected data field

UIN (?): 9C600000000001 detected on 11/12/18 09:17:14 UTC
Message type: distress / long
Protocol: user
Registered in: France (MID=227)
Orbitography Protocol
Orbitography data: 000000000001  (000000000000000000000000000000000000000000001)

UIN (?): 9C634E2AB509240 detected on 11/12/18 09:17:31 UTC
Message type: distress / long
Protocol: user
Registered in: France (MID=227)
Orbitography Protocol
Orbitography data: 34E2AB509240  (110100111000101010101101010000100100100100000000)
```



```
EPIRB TEST detected at : 18-05-11 10:48:24
UIN     : 4224C853012576F
  Format   : 0 (short)
  Protocol : 0 (location protocol)
  Country : 529 (KIR Kiribati)
User code : 2 EPIRB - MMSI/Location Protocol
MMSI : 418264 bcn : 0
Location source external
121.5 MHz homing
Location : S18°30' 00" W21°45' 00" (+/-15')

bps 401.3
```







SARSAT Satellites

- GOES
- GPS
- GALILEO
- GLONASS-K
- FENGYUN
- INMARSAT
- INSAT
- ELECTRO-L

- NOAA
- METOP
- NPOESS
- BEIDOU
- DASS

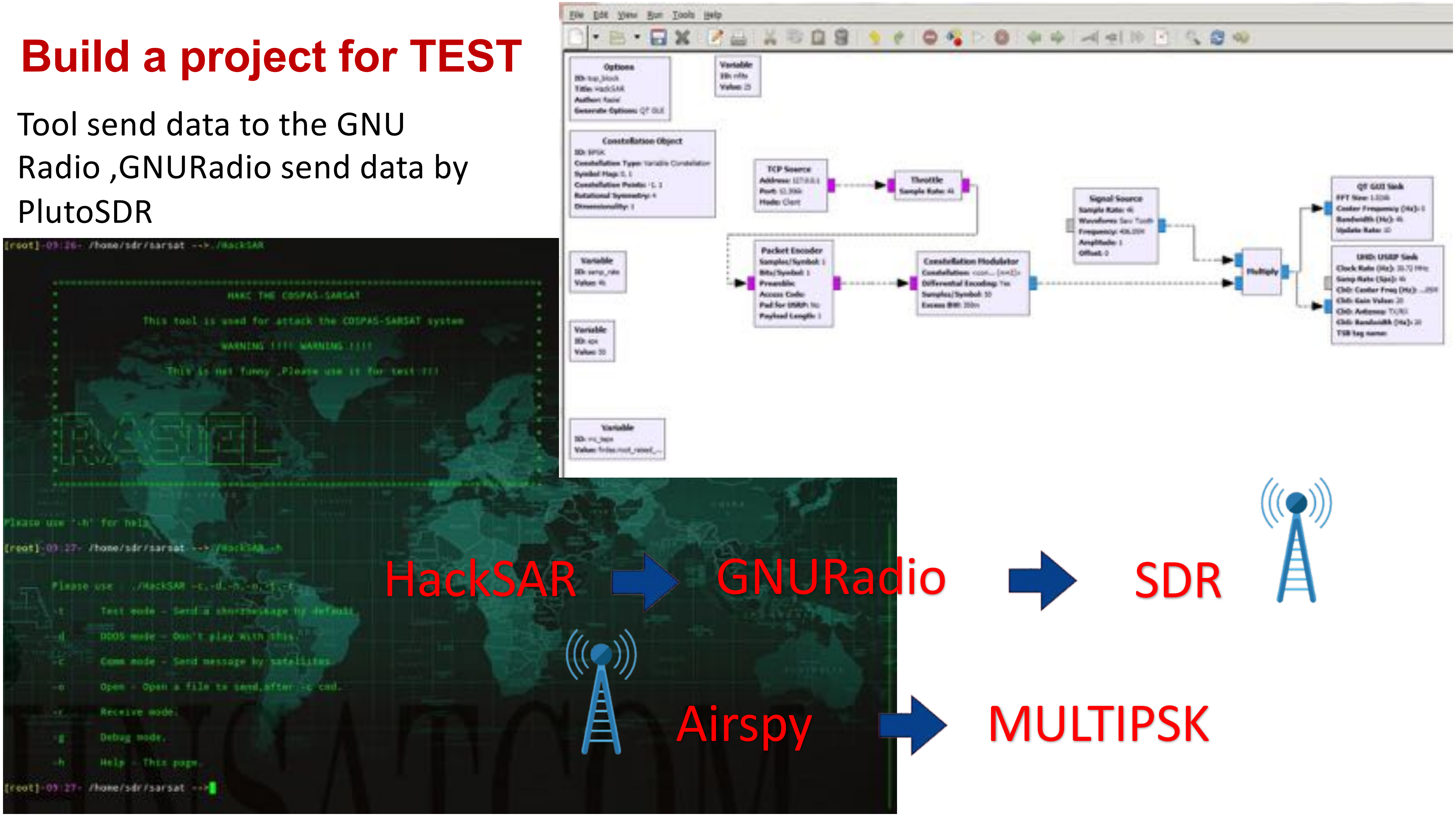
…

- More than 2,000,000 users
- 67 satellites online now
- 94 LUT stations
- 34+ MCC control centers

Let’s do a loopback test ！

Build a project for TEST

Tool send data to the GNU Radio ,GNURadio send data by PlutoSDR



```
[root]-09:26- /home/sdr/sarsat -->./HackSAR

    ************************************************************
    *                  HAKC THE COSPAS-SARSAT                  *
    *                                                          *
    *     This tool is used for attack the COSPAS-SARSAT system *
    *                                                          *
    *              WARNING !!!! WARNING !!!!                   *
    *                                                          *
    *        This is not funny ,Please use it for test !!!     *
    *                                                          *
    *  RASTEL                                                  *
    ************************************************************

Please use '-h' for help

[root]-09:27- /home/sdr/sarsat -->./HackSAR -h

    Please use   ./HackSAR -c,-d,-h,-o,-t,-r

    -t        Test mode - Send a shortmessage by default.
    -d        DDOS mode - Don't play with this.
    -c        Comm mode - Send message by satellites.
    -o        Open - Open a file to send,after -c cmd.
    -r        Receive mode.
    -g        Debug mode.
    -h        Help - This page.

[root]-09:27- /home/sdr/sarsat -->
```

Options
ID: top_block
Title: HackSAR
Author: Rastel
Generate Options: QT GUI

Variable
ID: nfilts
Value: 25

Constellation Object
ID: BPSK
Constellation Type: Variable Constellation
Symbol Map: 0, 1
Constellation Points: -1, 1
Rotational Symmetry: 4
Dimensionality: 1

TCP Source
Address: 127.0.0.1
Port: 52,001
Mode: Client

Throttle
Sample Rate: 4k

Variable
ID: samp_rate
Value: 4k

Packet Encoder
Samples/Symbol: 1
Bits/Symbol: 1
Preamble:
Access Code:
Pad for USRP: No
Payload Length: 1

Constellation Modulator
Constellation: <con... (n=2)>
Differential Encoding: Yes
Samples/Symbol: 10
Excess BW: 350m

Variable
ID: sps
Value: 10

Variable
ID: rrc_taps
Value: firdes.root_raised_...

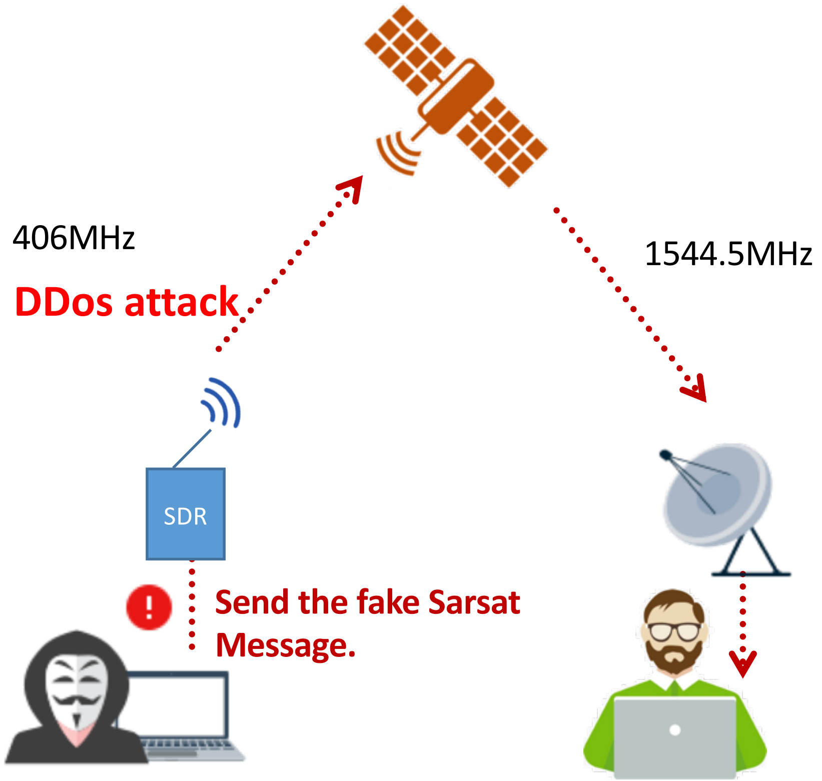
Signal Source
Sample Rate: 4k
Waveform: Saw Tooth
Frequency: 406.00M
Amplitude: 1
Offset: 0

Multiply

QT GUI Sink
FFT Size: 1.024k
Center Frequency (Hz): 0
Bandwidth (Hz): 4k
Update Rate: 10

UHD: USRP Sink
Clock Rate (Hz): 30.72 MHz
Samp Rate (Sps): 4k
Ch0: Center Freq (Hz): ...00M
Ch0: Gain Value: 20
Ch0: Antenna: TX/RX
Ch0: Bandwidth (Hz): 20
TSB tag name:

Actually achievable

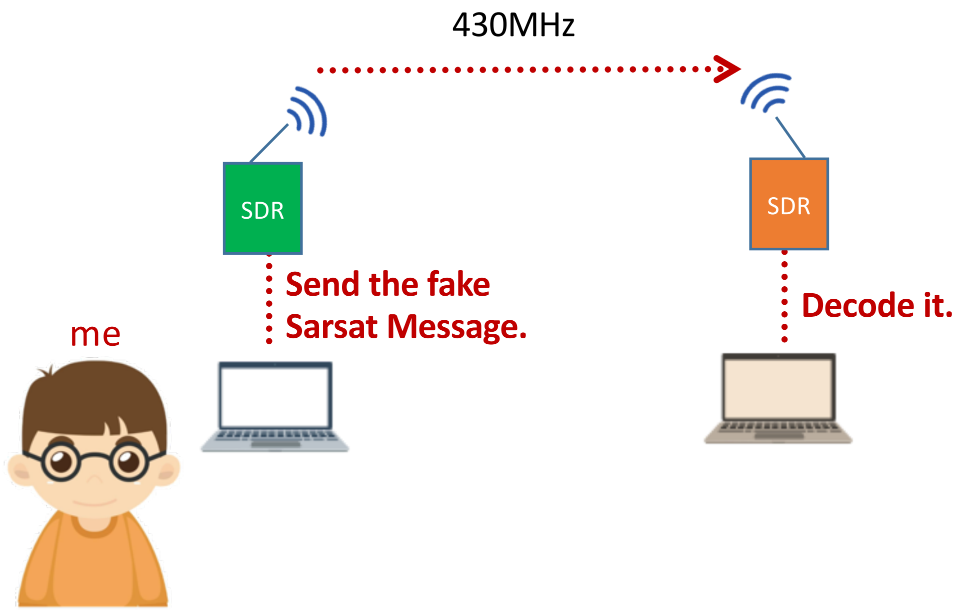


DDos attack

Send the fake Sarsat Message.

Receive the false Sarsat message.

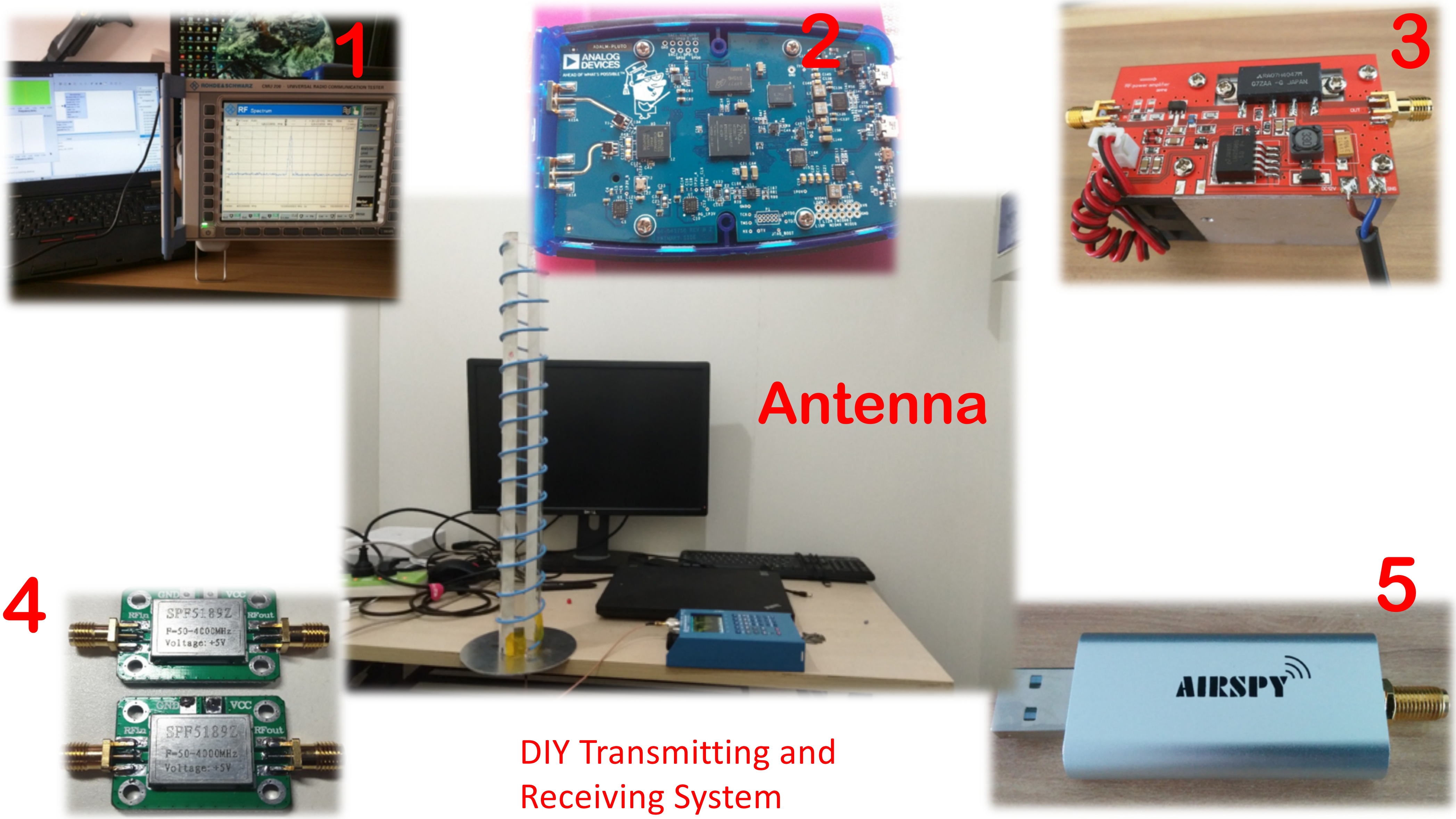
Actually test



Send the fake Sarsat Message.

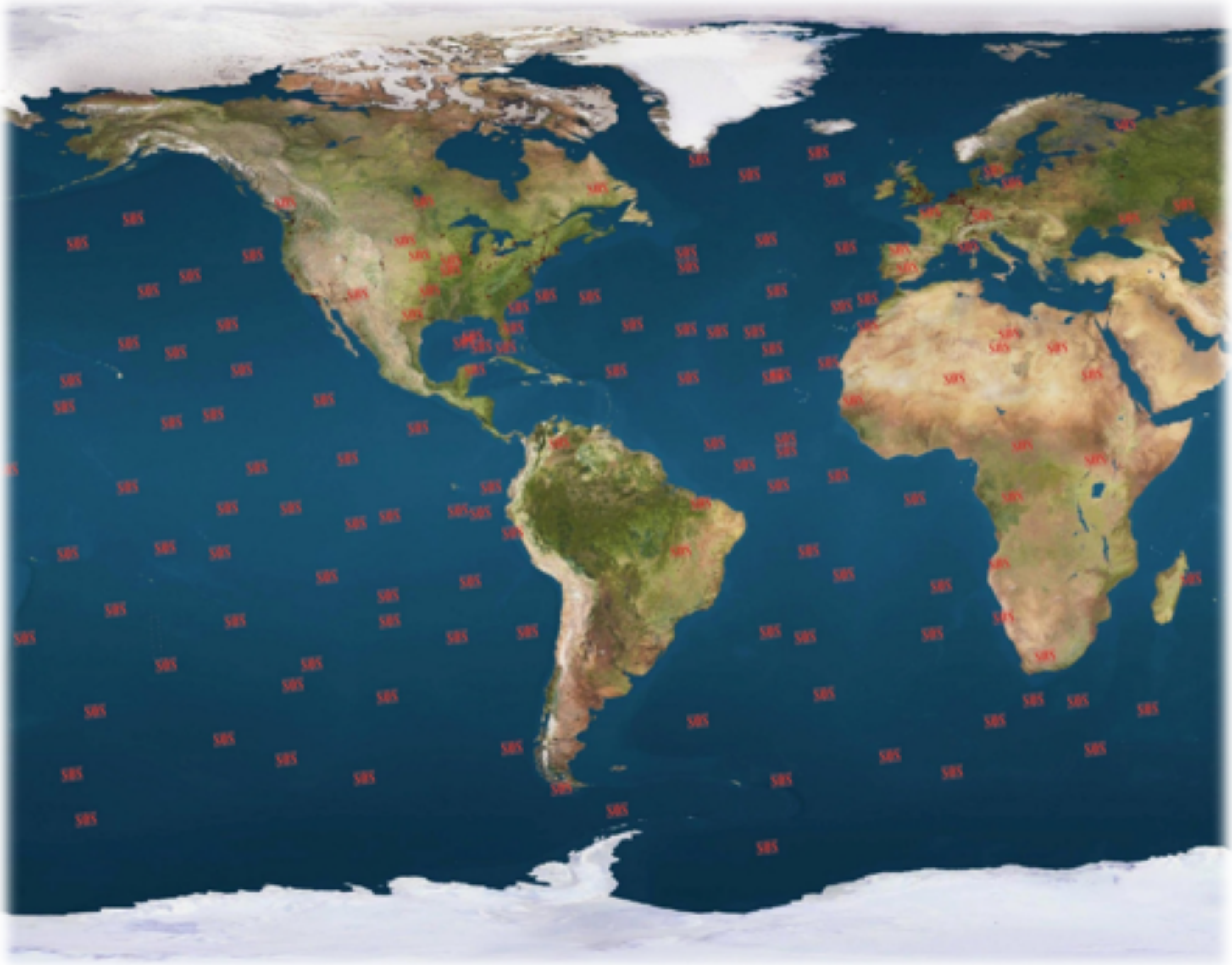
Decode it.

The test was operated at 430 MHz, so it did not affect the satellites.



DIY Transmitting and Receiving System

What impact does this vulnerability have?



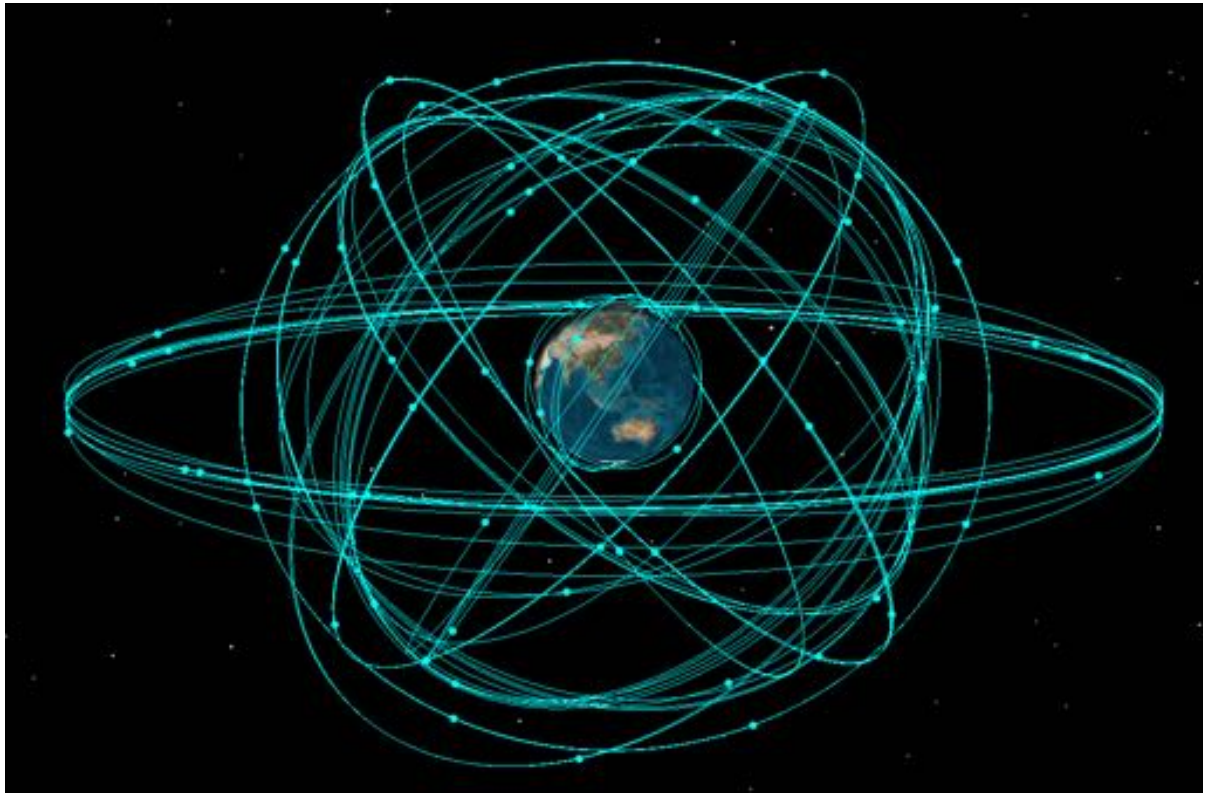
If someone attack one of the satellites, he will attack the entire SARSAT system around the world.

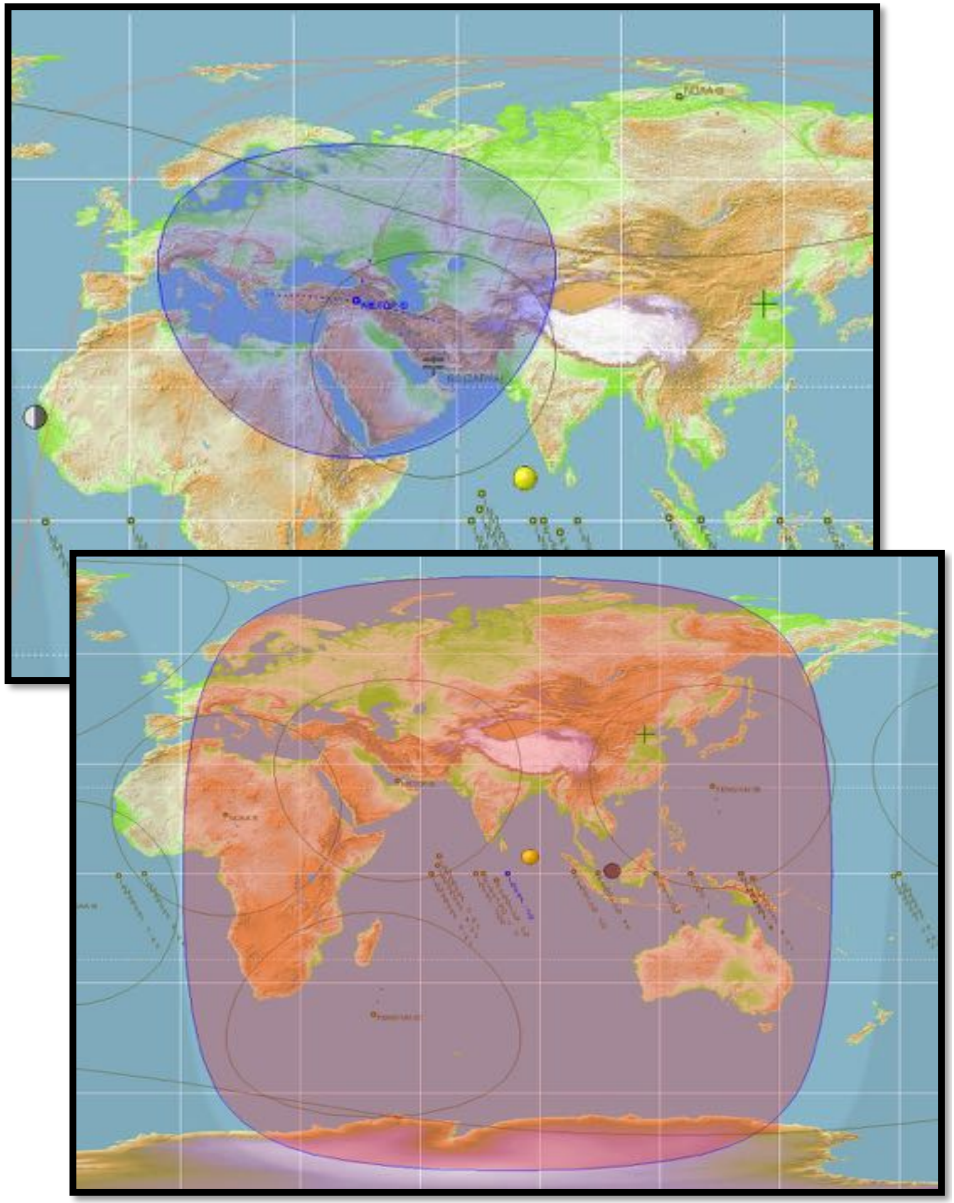
If someone is using the illegal machines to send information through the SARSAT satellites, he can even use his own modulation and encryption. Only one intercom can decode out information.

Interphone mode

007 mode

Spy Machine



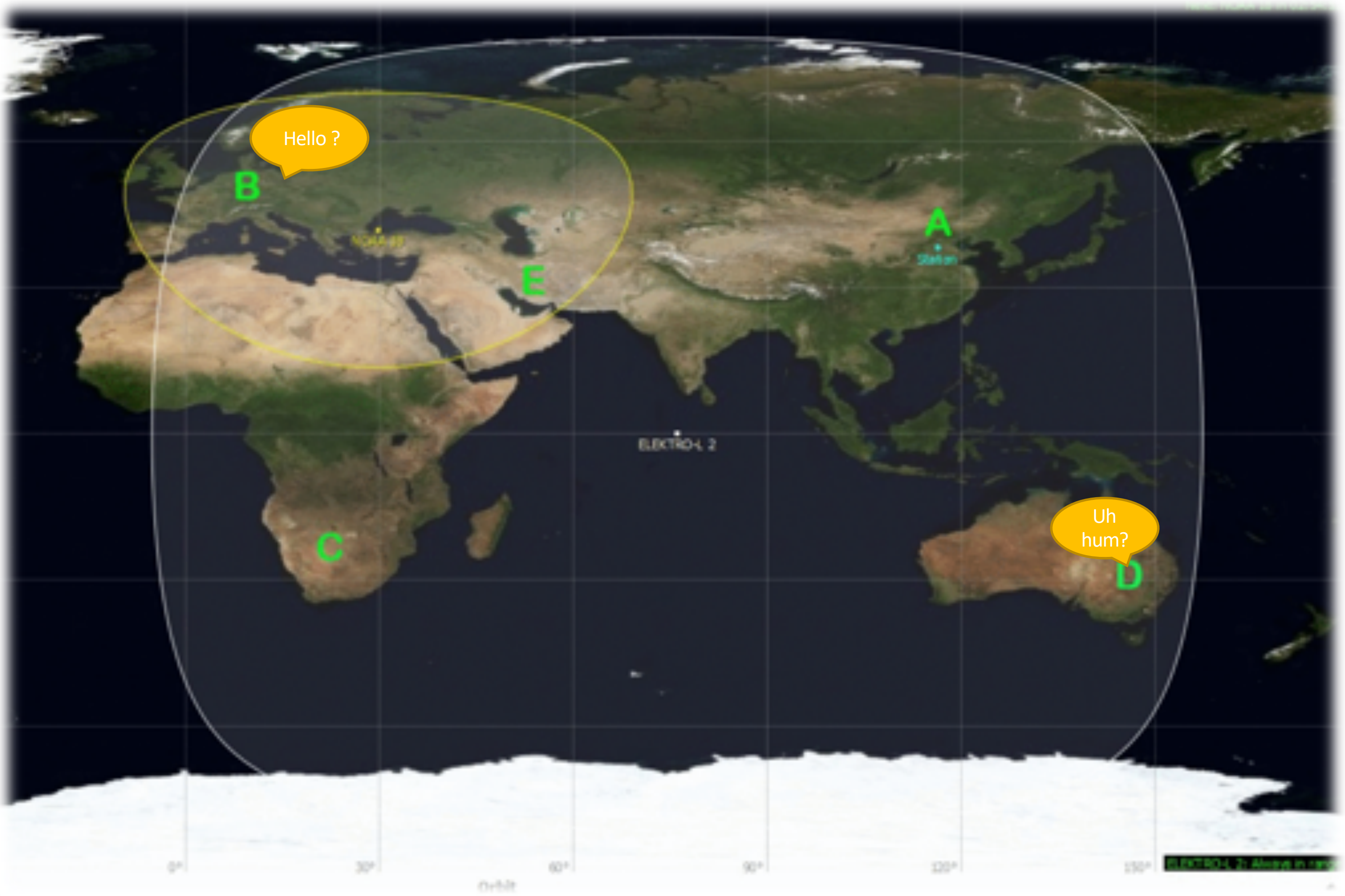


67 SARSAT satellites in the air

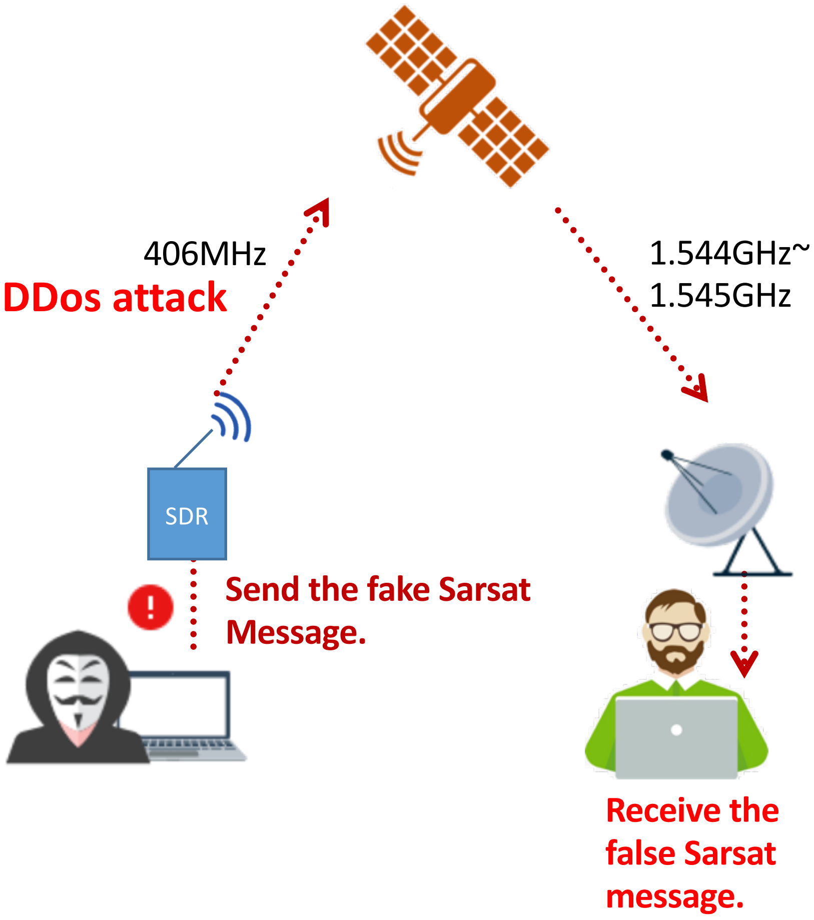
If B in Germany sends a message via satellite ELEKTRO-L2, D can receive it in Australia.

They can use satellites as repeaters to send their own encrypted and modulated messages.

Maybe spy already using it !



DDos Attack



406MHz

DDos attack

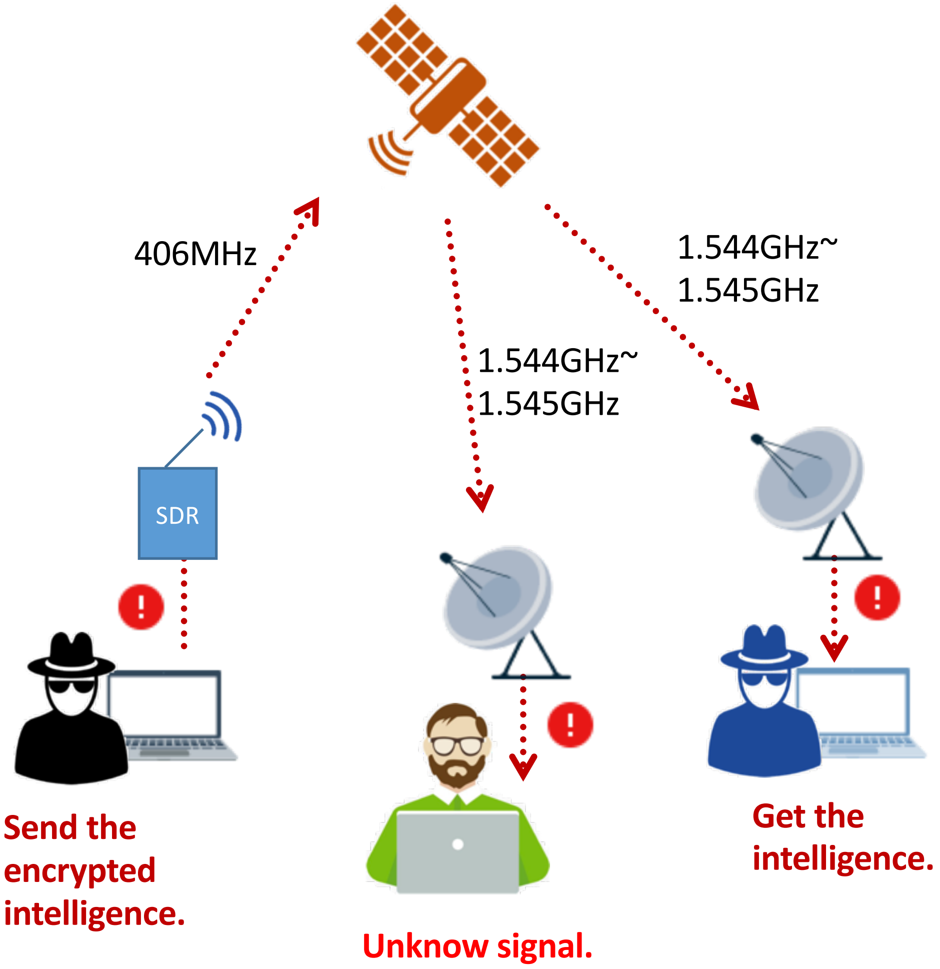
SDR

Send the fake Sarsat Message.

1.544GHz~ 1.545GHz

Receive the false Sarsat message.

Stealing links



406MHz

SDR

Send the encrypted intelligence.

1.544GHz~ 1.545GHz

Unknow signal.

1.544GHz~ 1.545GHz

Get the intelligence.

Blocking interference calculation

Satellite receiver designed for high sensitivity(about -160dBm), the receive level range for SARP and SARR is： -164~-137dBw, we set up a typical 406MHz high-power radio with a transmit power of 30W(44.77dBm), the orbital altitude of NOAA-19 is 865km,we calculate it based on the free space loss formula：

$$Ls = 32.45+20x\log 865+20x\log 406=143.36dB$$

The signal level to the satellite is：

$$44.77dBm-143.36dB= -98.59dBm = -128.59dBw$$

The max signal level of the payload is -137.2dBw, that will cause the load to receive blocking interference ,unable to receive beacon from terminal.

The min signal level can be received is: -160dBm+143.36dB= -16.64dBm

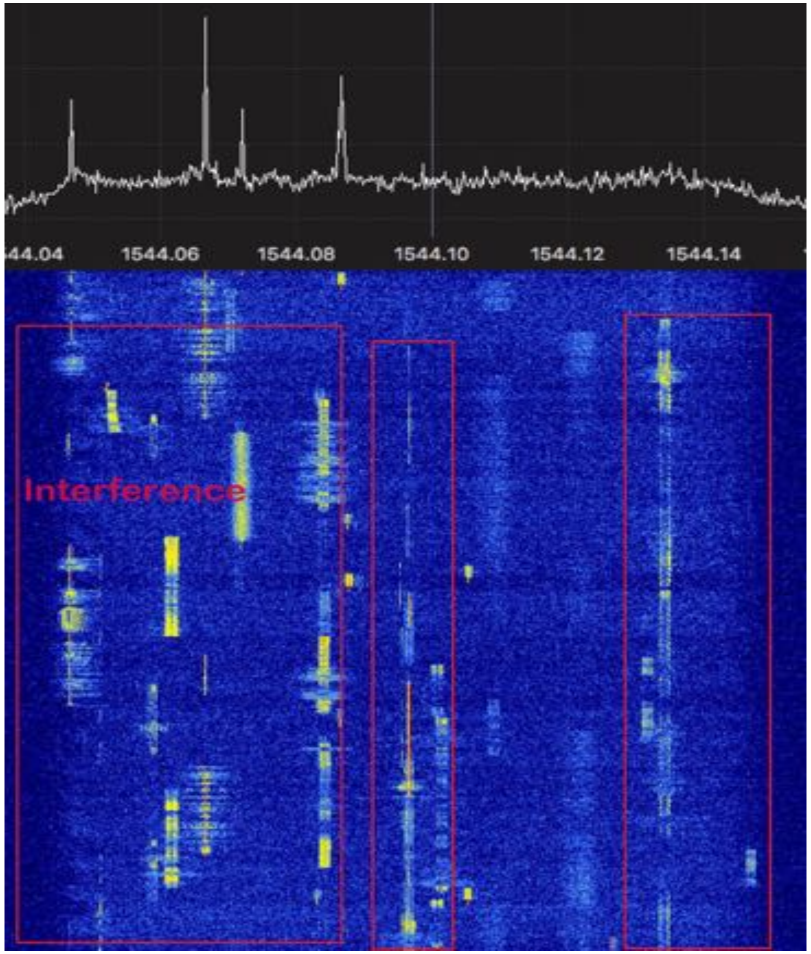
Anyway ,that's will cause interference to polar orbiting satellites more than -16.64dBm power.

Conclusion

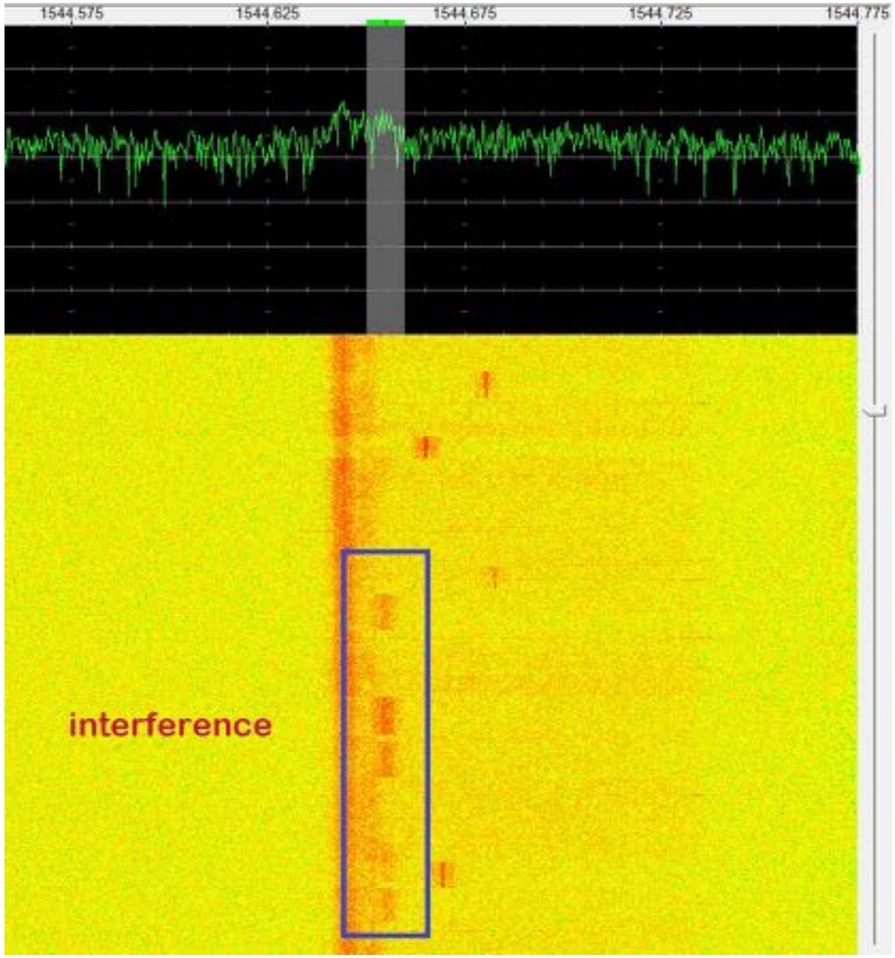
- Anyone can receive and decode messages through the L-band antenna.
- The satellite payload is too sensitivity , very easy to interference and DDOS attacks.
- Everyone can send false message to the satellite.

- The satellite link can be stolen.

So much interference



Australia



England

It is illegal to transmit information on 406MHz !!!

Most intercoms can be sent and receive at 400~470MHz.

This is why so many interferences can be found in the downlink of the satellites.

My friend helped me to record some signal in Australia, UK and the US. We can see that the system is very common interference.

I want to say :

Please do not interfere this system,
We need this system to save more people.
They are saving our lives.

Thanks

@uhf_satcom @sam210723

- COSPAS-SARSAT: https://cospas-sarsat.int/en
- Register your beacon: https://www.406registration.com
- 360 Technology Home page: https://www.360.cn
- My home page: http://www.chnsatcom.com
- Twitter: Rasiel_J

Q&A ?