International GNSS Summer School 2019

Organized by Tokyo University of Marine Science and Technology

Course

Module A: GNSS Signal Security
Module B: Spoofing & GNSS Signal Authentication
Module C: Android GNSS Raw Data Processing

Dinesh MANANDHAR
Center for Spatial Information Science
The University of Tokyo
dinesh@iis.u-tokyo.ac.jp

29th July – 3rd August 2019, Tokyo

- Dinesh Manandhar
- Associate Professor (Project), Center for Spatial Information Science, The University of Tokyo
- Adjunct Associate Professor, Asian Institute of Technology, Thailand
- Member, ISO/TC-204, WG18
- Member, ICAO/NSP, DFMC/SBAS Signal Authentication

Outline of the Lecture

- **Module A: GNSS Signal Security**
  - **Introduction to GNSS Vulnerabilities**
    - **Interference**
    - **Jamming**
    - **Spoofing**
- **Module B: Spoofing and GNSS Signal Authentication**
  - **Detail discussions on Spoofing**
  - **Demonstration of Spoofing**
  - **Anti-Spoofing Methods**
  - **Demonstration of Anti-Spoofing Method**
- **Module C: Android GNSS Raw Data Processing**
  - **Introduction**
  - **Android Devices**
  - **Data Logging Tools**
  - **Data Processing Tools**
  - **Data Processing Outputs**
  - **Innovative and Challenging Applications**

Module – A
GNSS Signal Security

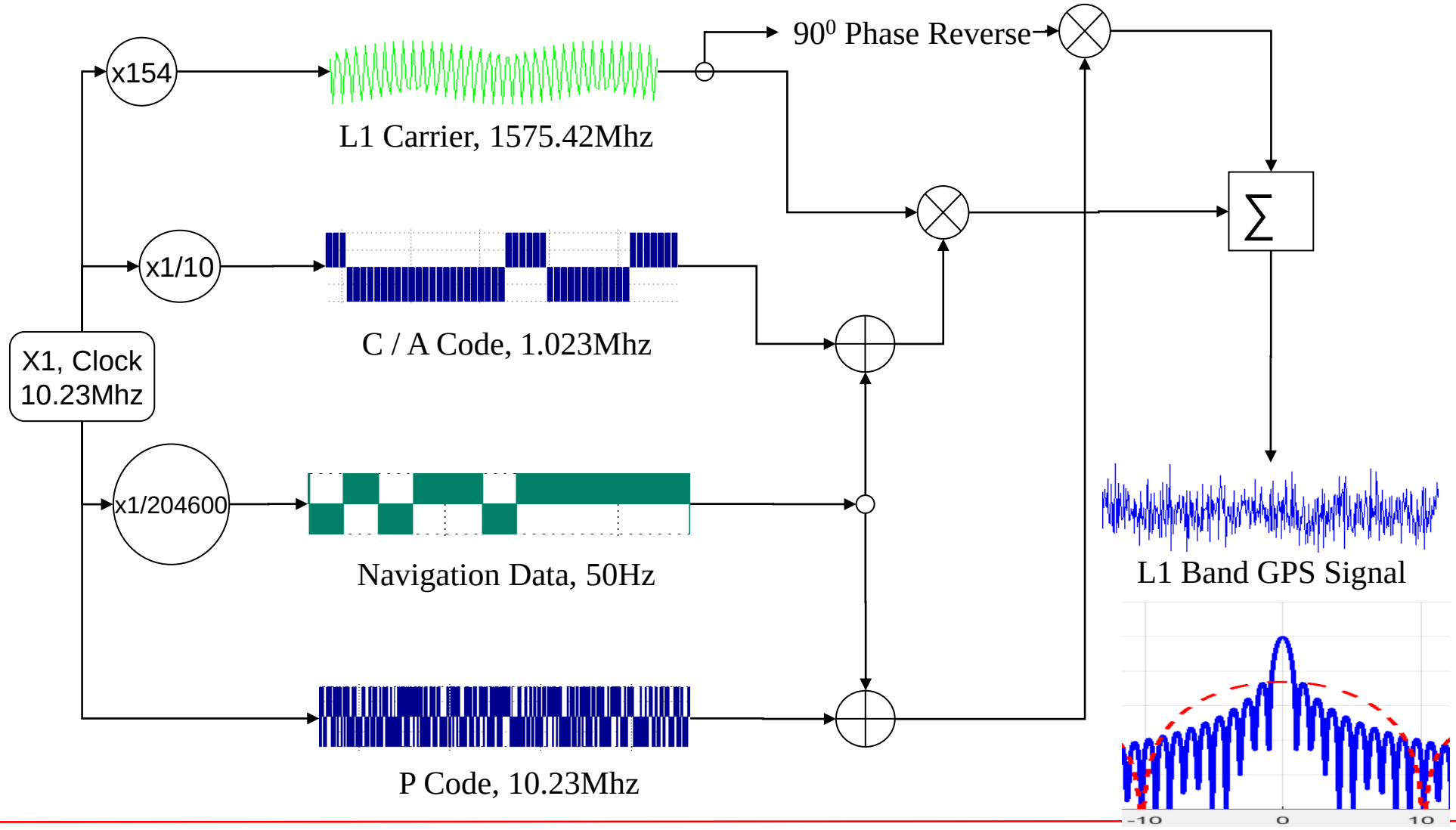
Module – A : Contents

- **Background Information**
  - **GPS Signal Structure**
  - **Correlation and Cross-Correlation**
- **Signal Power**
- **Types of Interferences**
- **Jamming Issues**
- **Interference affected IF data samples**

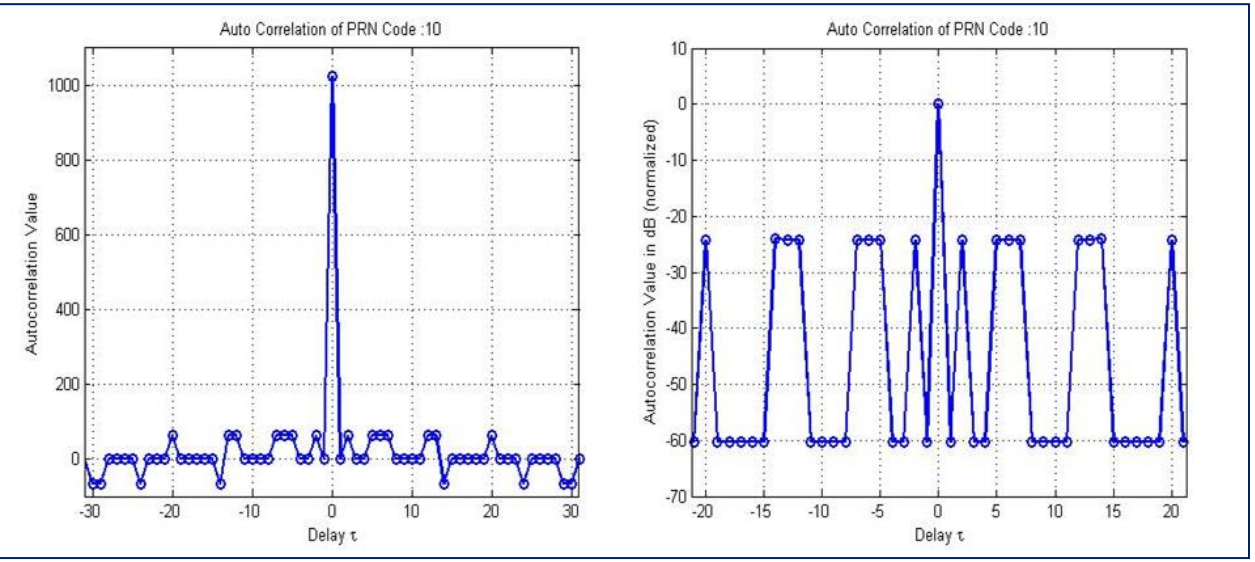
Introduction

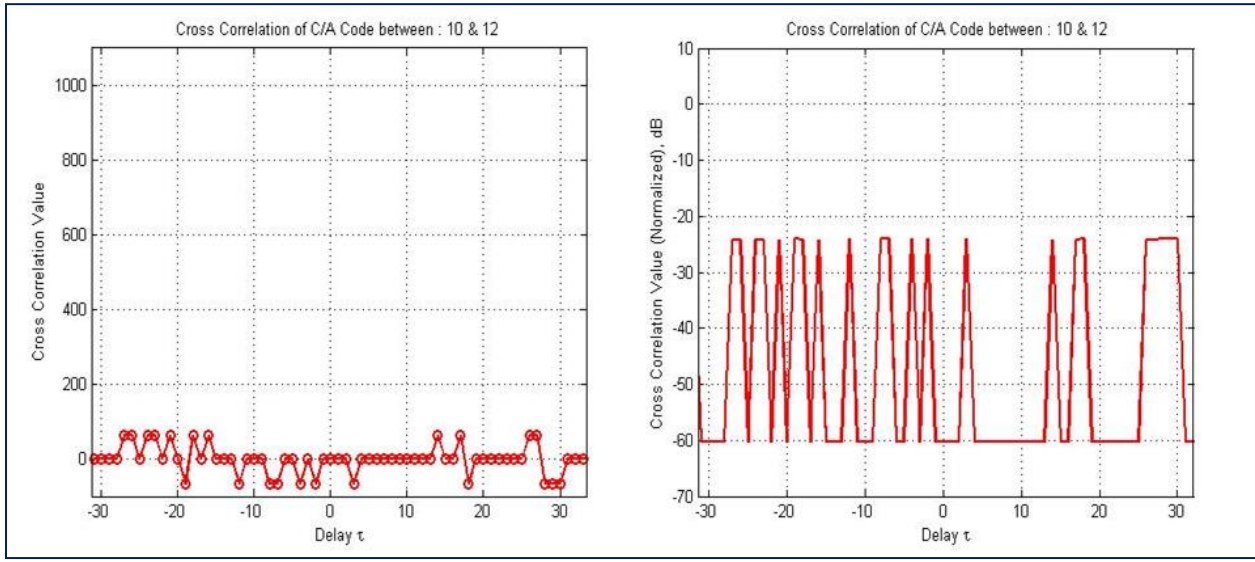
- **What is GNSS Signal Security?**
  - **This is about keeping the signals free from vulnerabilities like Jamming, Interference and Spoofing.**
  - **There are many guidelines, regulations, policies, laws related with Jamming and Interference**
  - **But, very little on Spoofing.**

Background Information : GPS Signal Structure



Background Information : Characteristics of PRN Code





Auto-correlation: Only four values 1023, 1, 63 or 65 (Ideal case)

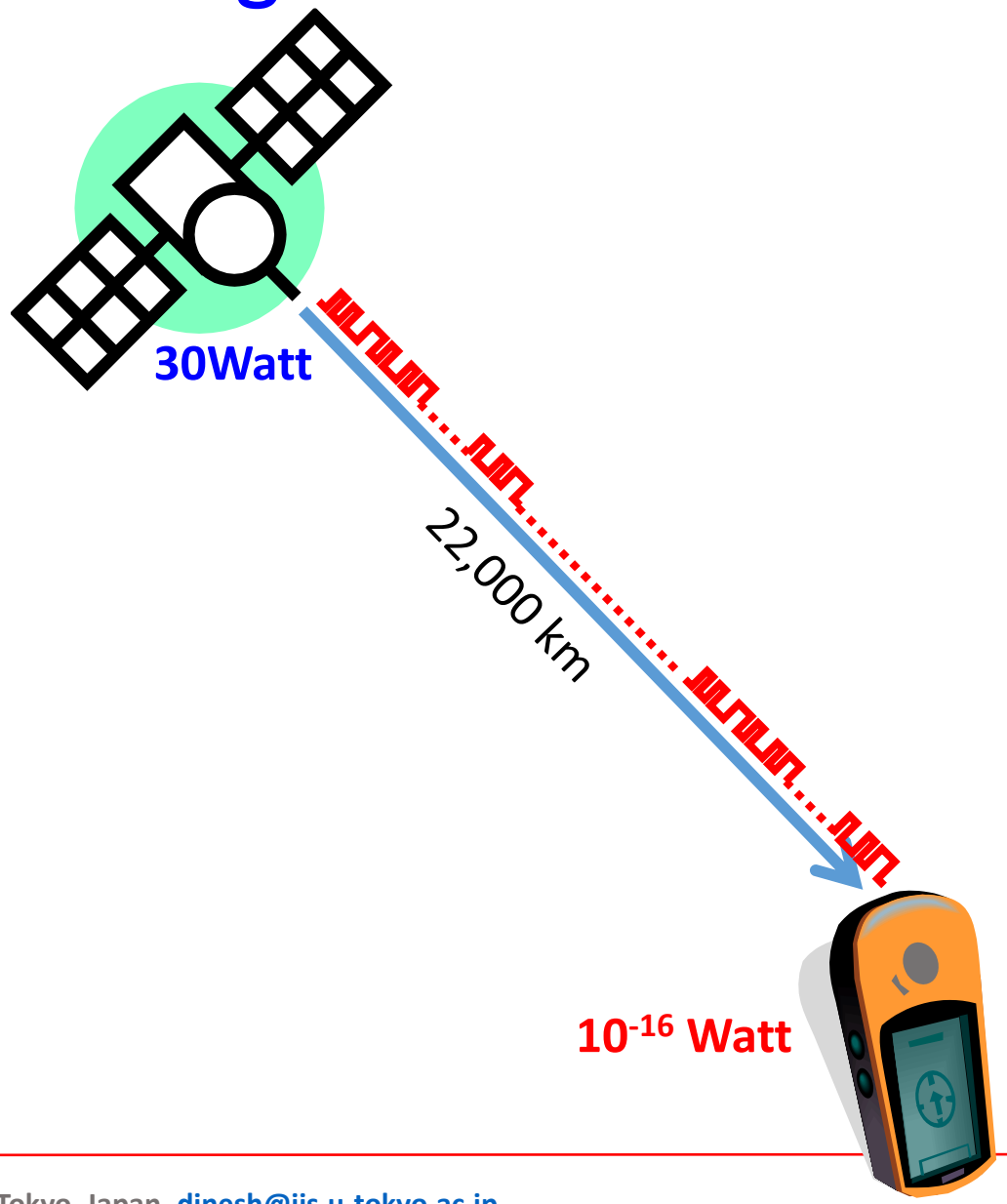
- PRN codes are very uniquely designed.
- GPS and other GNSS use CDMA
  - One PRN code is assigned to one satellite.
  - In case of GPS, PRN code is 1023 bits long.
  - GLONASS is different. It uses FDMA. The same code for all satellites but different frequencies.
  - Some new signals of GLONASS also uses CDMA signals

Cross-correlation: Only three values 1, 63 or 65 (Ideal Case)

- Maximum Cross-correlation Value is -23dB.
- If any signal above this power enters a GPS receiver, it will totally block all GPS signals.
- If longer PRN code is used, receiver becomes more resistive to Jamming signal
  - But, signal processing is more complex

GPS Signal Power: How Strong or How Weak?

- GPS satellites are about 22,000km away
- Transmit power is about 30W
- This power when received at the receiver is reduced by 10^{16} times.
  - The power reduces by 1/(distance)^2
  - This is similar to seeing a 30W bulb 22,000Km far away
- GPS signals in the receiver is about 10^{-16} Watt, which is below the thermal noise



GPS Signal Power: How Strong or How Weak?

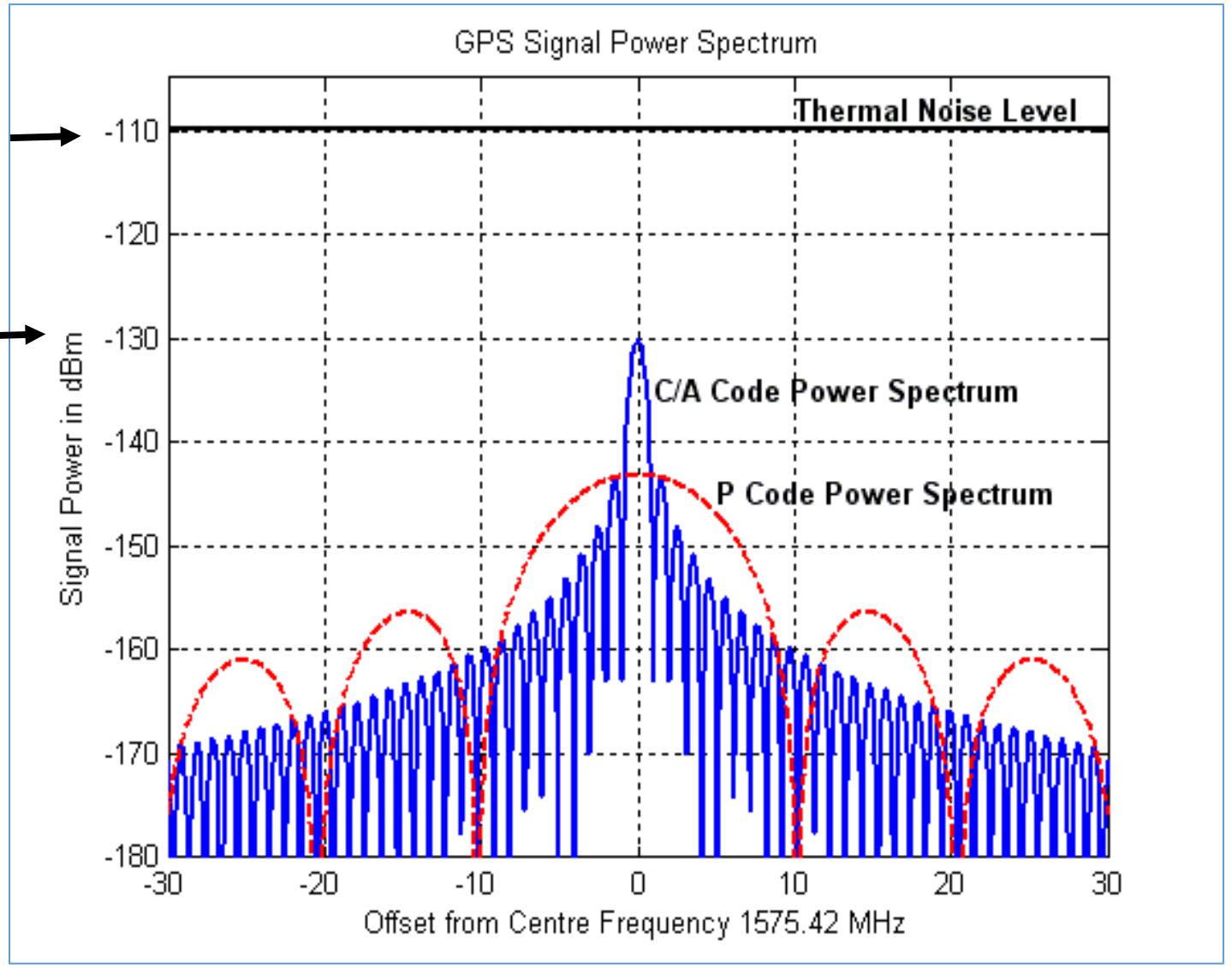
- **GPS Signal Power at Receiver**
  - **-130dBm or -160dBW**
- **Thermal Noise Power**
  - **Defined by $kT_{eff}B$, where**
    - $K = 1.380658e\text{-}23JK^{-1}$, Boltzman Constant
    - $T_{eff} = 362.95$, for Room temperature in Kelvin at 290
      - Teff is effective Temperature based on Frii's formula
    - $B = 2.046MHz$, Signal bandwidth
  - **Thermal Noise Power = -110dBm for 2MHz bandwidth**
  - **If Bandwidth is narrow, 50Hz**
    - Noise Power = -156dBm

GPS Signal Power

Noise Power
Any Signal below this noise level can't be measured in a Spectrum Analyzer

GPS Signal Power at Antenna
-130dBm

Mobile phone, WiFi, BT etc have power level above -110dBm, much higher than GPS Signal Power



Power of GPS vs. Other Signals

	Signal Type	Power (based on calculations, not measured)		
		Watt	dBW	dBm
Above Noise	Mobile Phone Handset TX Power *	1W	0dBW	30dBm
	Power at Mobile Phone Handset*	100e-6W	-40dBW	-70dBm
	ZigBee	316e-16W	-115dBW	-85dBm
	VHF	200e-16W	-137dBW	-107dBm
	Thermal Noise	**79e-16W**	**-141dBW**	**-111dBm**
Below Noise	GPS**	**1e-16W**	**-160dBW**	**-130dBm**

- * Actual power values will differ. These are just for comparison purpose
- ** GPS Signals are hidden under the noise. Thus, it can't be measured directly e.g. using a Spectrum Analyzer

Consequences of Different Power Levels

- **The large power difference between GNSS and other signal levels make GNSS receivers comparatively more susceptible to interference**
  - **Mobile network devices are able to raise power levels to cope with obstructions and poor radio environments.**
  - **But, GNSS signal power levels are fixed**

- **If GNSS signals shared frequencies with mobile systems, they would be swamped by interference**
  - **GNSS reception would not be possible**

Source: UN-Nepal GNSS Workshop, IDM Session

Types of Interference

- **Self-Interference**
  - **Interference from GPS like signals**
    - Interference from Pseudolites or GPS like signals to GPS (same frequency and similar signals)
    - See Characteristics of PRN Code Slide
- **In-band Interference**
  - **Different frequency but within the bandwidth of GNSS signals**
    - E.g. GPS L1C/A signal bandwidth is +/- 10MHz. Any signal with frequency within 1565MHz – 1585MHz may have in-band interference.
- **Out-Of-Band Emission (OOBE)**
  - **Different frequency outside of the bandwidth of GNSS signals**
    - E.g. GPS L1C/A signal bandwidth is +/- 10MHz. Even if a signal is outside of 1565MHz – 1585MHz range, the signal may still interfere GNSS signal due to spurious or harmonics that's falling within the GNSS signal's frequency bandwidth
- **Spurious emission**
    - Harmonic vs Intermodulation Products
- **Adjacent band interference**
  - **Signals that have frequency near the GNSS signal's frequency bandwidth**

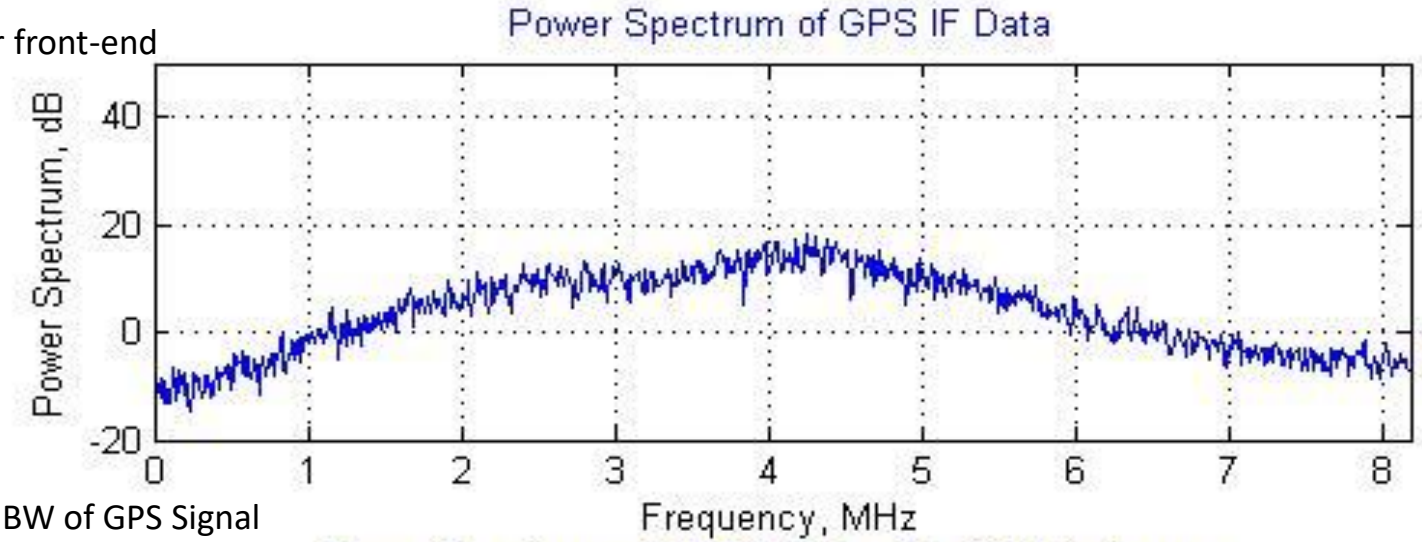
Source: UN-Nepal GNSS Workshop, IDM Session

In-Band Interference from GPS like Signals

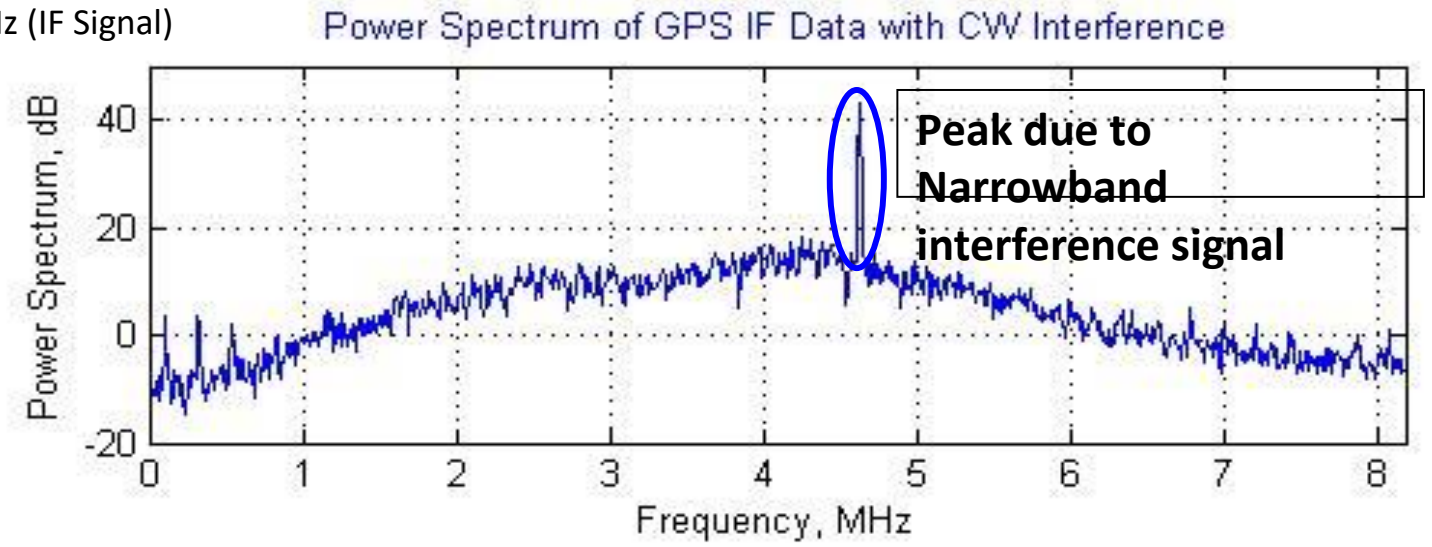
- **Interference from GPS like Signals**
  - **Pseudolites, GPS Signal Generators**
  - **It causes interference unless the transmit power is limited within the allowed level**
  - **In Japan, allowed maximum power level for license free weak signal is -64dBm at the antenna (EIRP) at 1575 Mhz.**
  - **If a Pseudolite transmit power at antenna is -64dBm**
    - It will completely affect all GPS receivers within 3-5m
    - It will affect the C/No value of GPS receiver within 10m
    - This is just theoretical guideline, Actual values differs a lot depending upon location, signal type etc
      - Values calculated from [Rx = Tx-a1-20*log10(d)] where, Rx is received power at distance d, Tx is transmit power, a1 = 36dB attenuation in one meter for GPS L1 frequency.

In-Band CW Interference

Interference free signal
IF Signal from a software receiver front-end
IF = 4.13Mhz



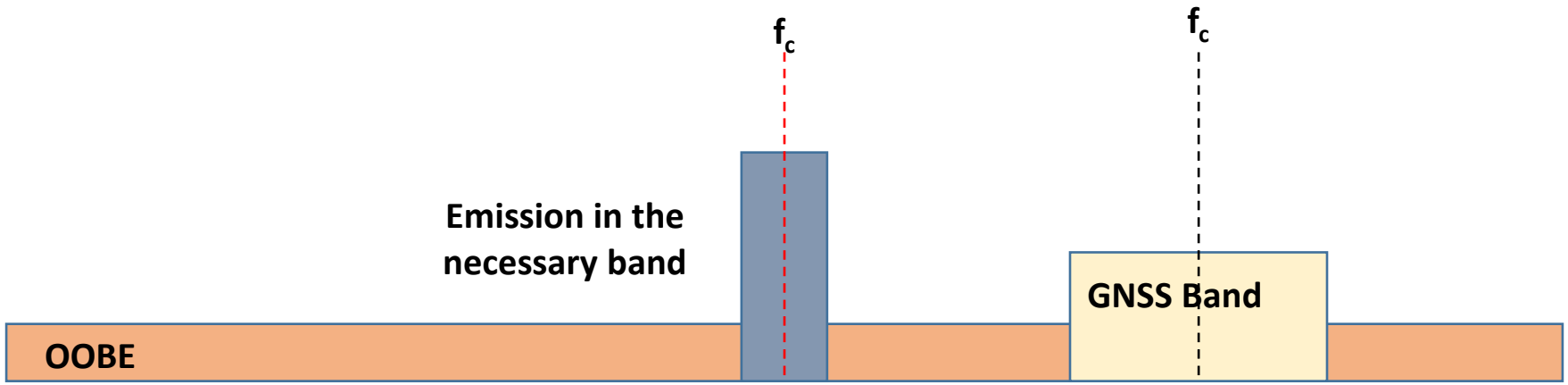
CW interference within the 2MHz BW of GPS Signal
The center frequency is at 4.13MHz (IF Signal)



CW: Continuous Wave produces narrow band signal

Out-Of-Band Emission (OOBE)

- **Out-of-band emission is an emission on a frequency or frequencies immediately outside the necessary bandwidth which results from the modulation process, but excludes spurious emissions**
- **It raises the noise floor of the GNSS receivers and the Carrier signal-to-Noise ratio (CNR) is reduced, impacting GNSS receiver performance**



Source: UN-Nepal GNSS Workshop, IDM Session

Spurious Emission

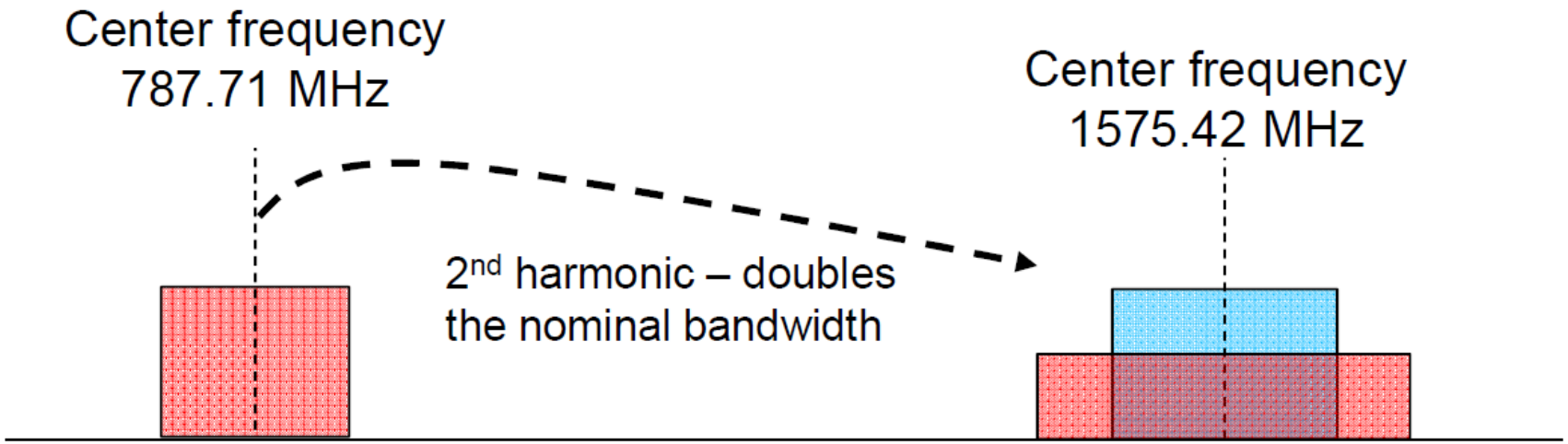
- **Spurious emission is an emission not deliberately created or transmitted on a frequency or frequencies which are outside the necessary bandwidth**

- **Examples include harmonic emissions and intermodulation products**

Source: UN-Nepal GNSS Workshop, IDM Session

Harmonic Emission

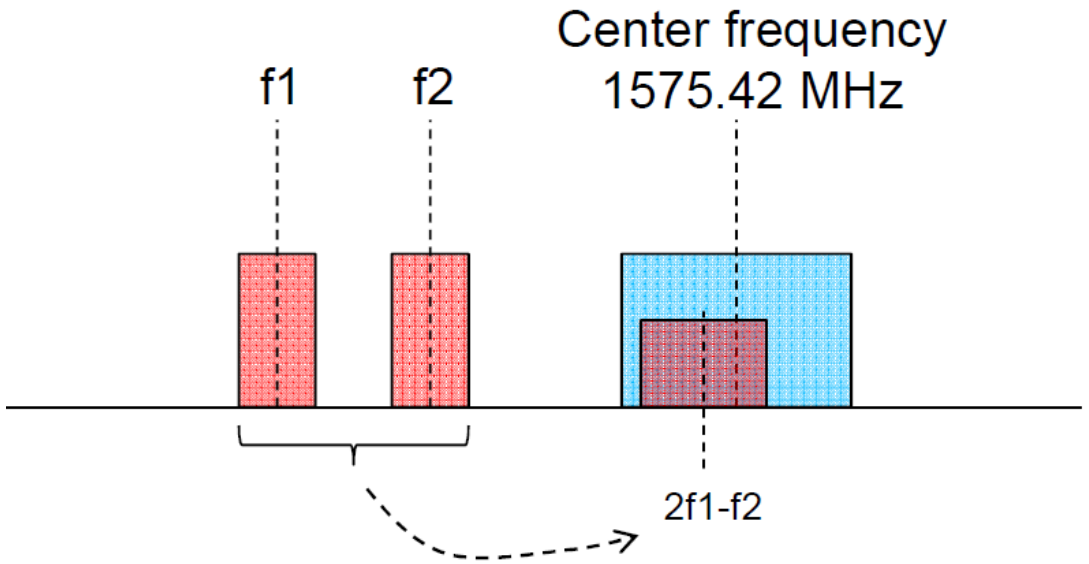
- ***N*-th harmonics for a signal whose fundamental frequency is *f*, has a frequency *N*f***
- **Generally not a significant interference mechanism**



Source: UN-Nepal GNSS Workshop, IDM Session

Intermodulation Emission

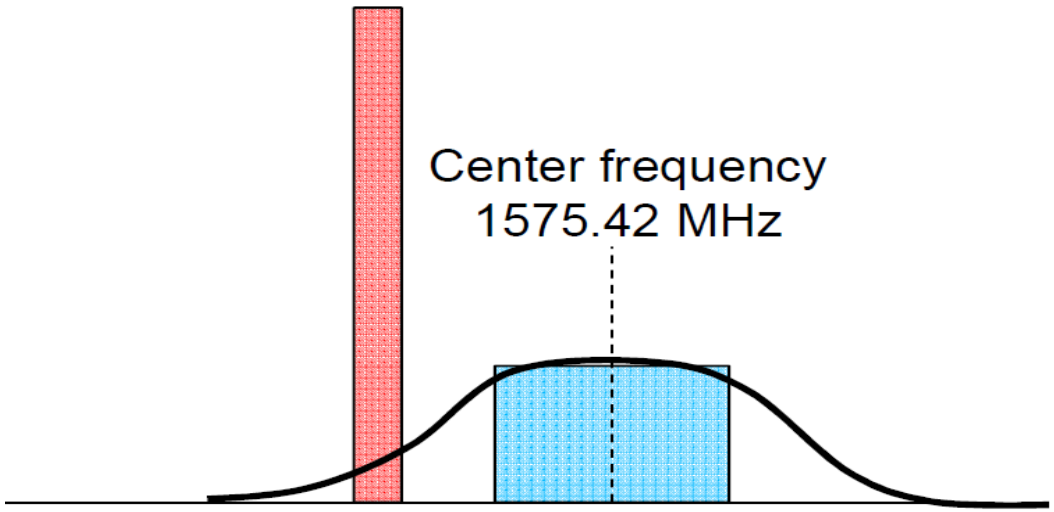
- **Intermodulation products is caused by amplitude modulation of signals containing two or more difference frequencies, caused by non-linearities in the front end of a GNSS receiver**
- **Intermodulation products can end up in the GNSS band and desensitize a GNSS receiver frontend**
- **Example: 3rd Intermodulation products from an adjacent band signal plan**



Source: UN-Nepal GNSS Workshop, IDM Session

Adjacent Band Interference

- **Applicable in cases when high powered "terrestrial" service is planned adjacent to the quiet "satellite" bands to create overload**
- **The frontend of the receiver is compressed or overloaded**
- **Front-end filtering can help reduce this effect which can be difficult with high power adjacent band source**



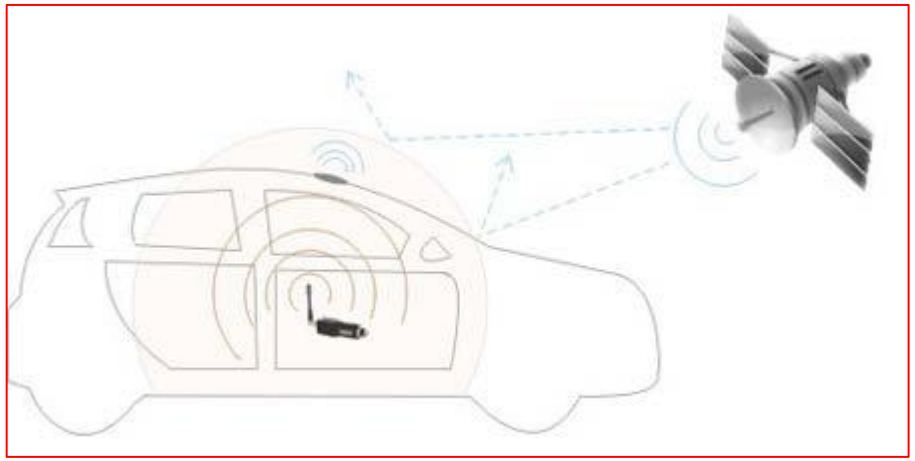
Source: UN-Nepal GNSS Workshop, IDM Session

GPS Jammers

Many handy type GPS Jammers exists.
They will jam not only your GPS but many others in the vicinity of few kilometers

Thousands using GPS jammers on UK roads pose risks, say experts : The Guardian

- https://www.theguardian.com/technology/2013/feb/13/gps-jammers-uk-roads-risks



https://www.jammer-store.com/gp5000-car-use-gps-jammer-blocker.html#

Jammers are illegal in the USA and many other countries

Major Enforcement Actions

- **May 2016:** FCC imposed a fine of $34,912,500 to a Chinese electronics manufacturer and online retailer for marketing 285 models of signal jamming devices to U.S. customers for more than two years.
  LEARN MORE (PDF) ➡
  AND MORE (PDF) ➡
- **August 2013:** FCC proposed a fine of nearly $32,000 for an individual whose illegal use of a GPS jamming device on the highway outside Newark Airport interfered with an aviation safety system in 2012.
  LEARN MORE (PDF) ➡
- **April 2013:** FCC fined two companies for using illegal signal jammers at their worksites. The fines were set at $144,000 and $125,000, respectively.
  LEARN MORE AT FCC.GOV ➡
  AND MORE ➡
- **October 2012:** FCC announced enforcement actions against individuals selling signal jamming devices on craigslist.org, warning that the Bureau intends to impose substantial monetary penalties for similar violations going forward.
  LEARN MORE AT FCC.GOV ➡
- **October 2011:** FCC announced it had issued 20 enforcement actions against online retailers in 12 states for illegally marketing more than 200 uniquely-described models of jamming devices.
  LEARN MORE AT FCC.GOV ➡

JAMMING CELL PHONES AND GPS EQUIPMENT IS AGAINST THE LAW!

In recent years, the number of websites offering "cell jammers" or similar devices designed to block communications and create a "quiet zone" in vehicles, schools, theaters, restaurants, and other places has increased substantially. While these devices are marketed under different names, such as signal blockers, GPS jammers, or text stoppers, they have the same purpose. We remind and warn consumers that it is a violation of federal law to use a cell jammer or similar devices that intentionally block, jam, or interfere with authorized radio communications such as cell phones, police radar, GPS, and Wi-Fi. Despite some marketers' claims, consumers cannot legally use jammers within the United States, nor can retailers lawfully sell them.

Why are jammers prohibited? Use of jamming devices can place you or other people in danger. For instance, jammers can prevent 9-1-1 and other emergency calls from getting through or interfere with law enforcement communications (ambulance, fire, police, etc). In order to protect the public and ensure access to emergency and other communications services, without interference, the FCC strictly prohibits the use, marketing, manufacture, and sale of jammers.

What happens if you use a jammer? Operation of a jammer in the United States is illegal and may subject you to substantial monetary penalties, seizure of the unlawful equipment, and criminal sanctions including imprisonment.

Want to file a complaint or need more information? To file a complaint alerting the FCC's Enforcement Bureau to illegal cell, GPS, or other jamming devices, please visit www.fcc.gov/complaints or call 1-888-CALL-FCC. Additional information about jammer enforcement is available at www.fcc.gov/eb/jammerenforcement or by emailing the Enforcement Bureau at jammerinfo@fcc.gov.

Issued by the Enforcement Bureau of the Federal Communications Commission

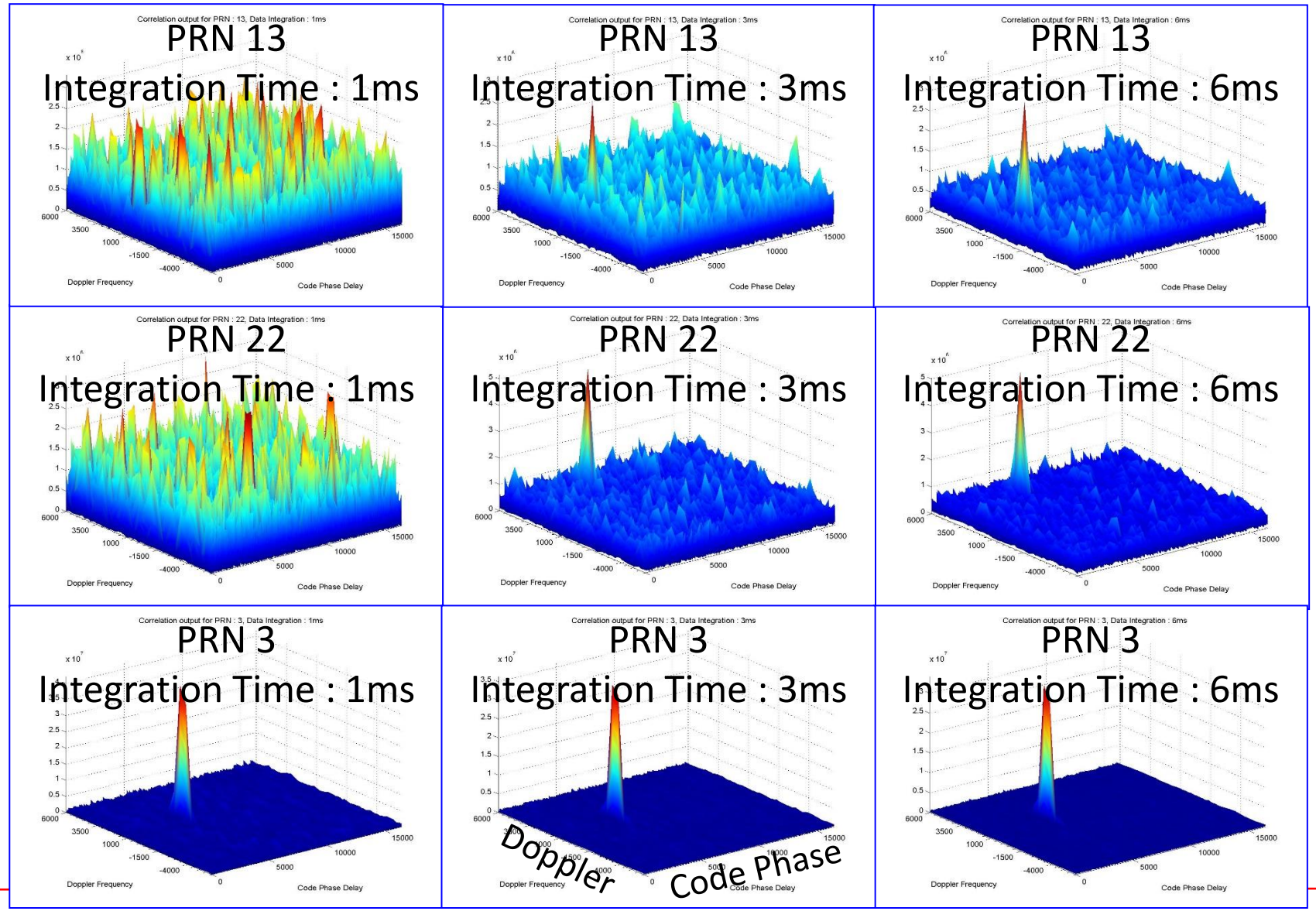
Source: http://www.gps.gov/spectrum/jamming/

Impact on Signal Processing due to Noise or Interference Signal

Presence of high level noise
This requires longer integration of data
More processing power

Presence of noise

Very small noise

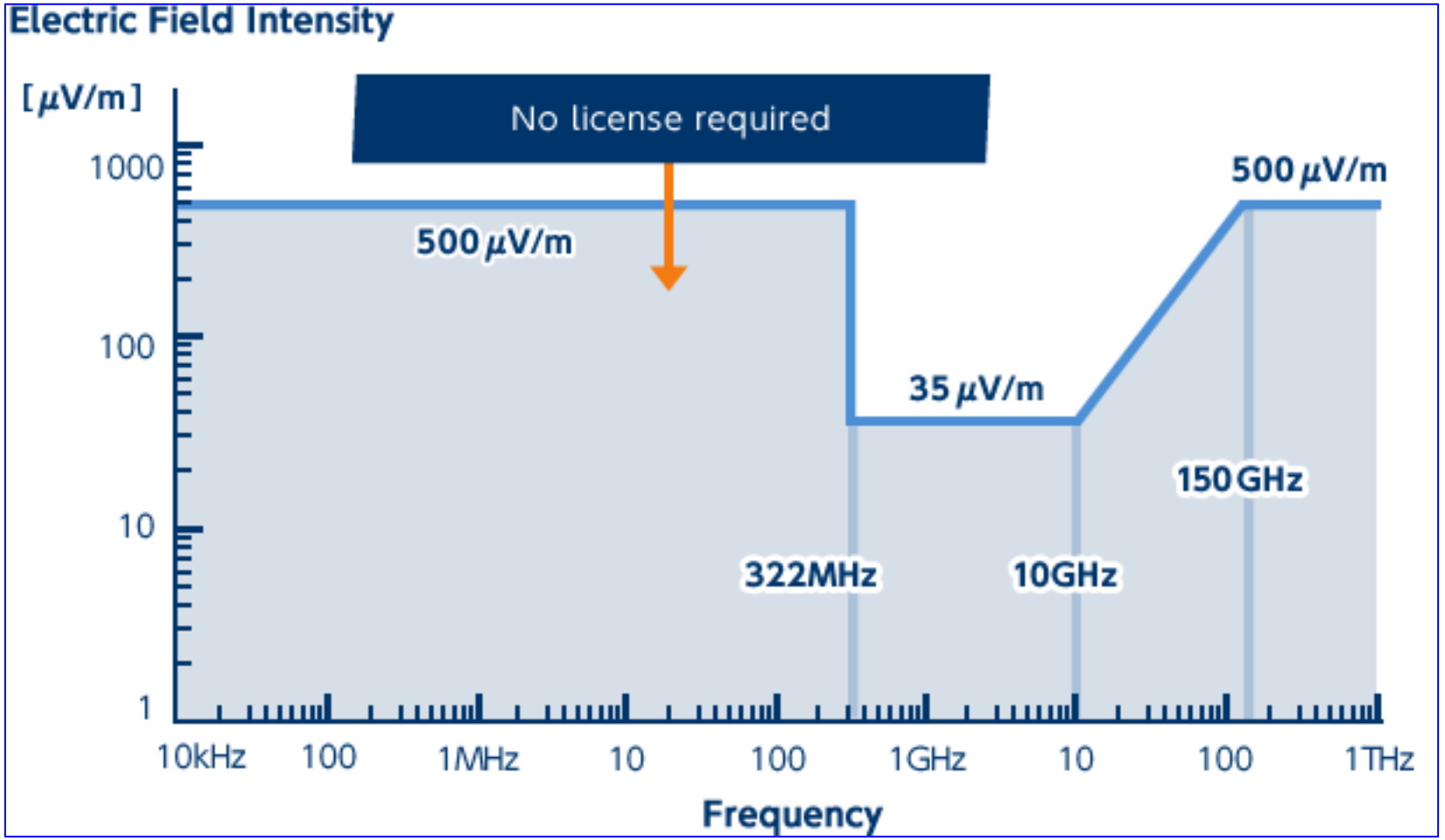


Interference Control Mechanism

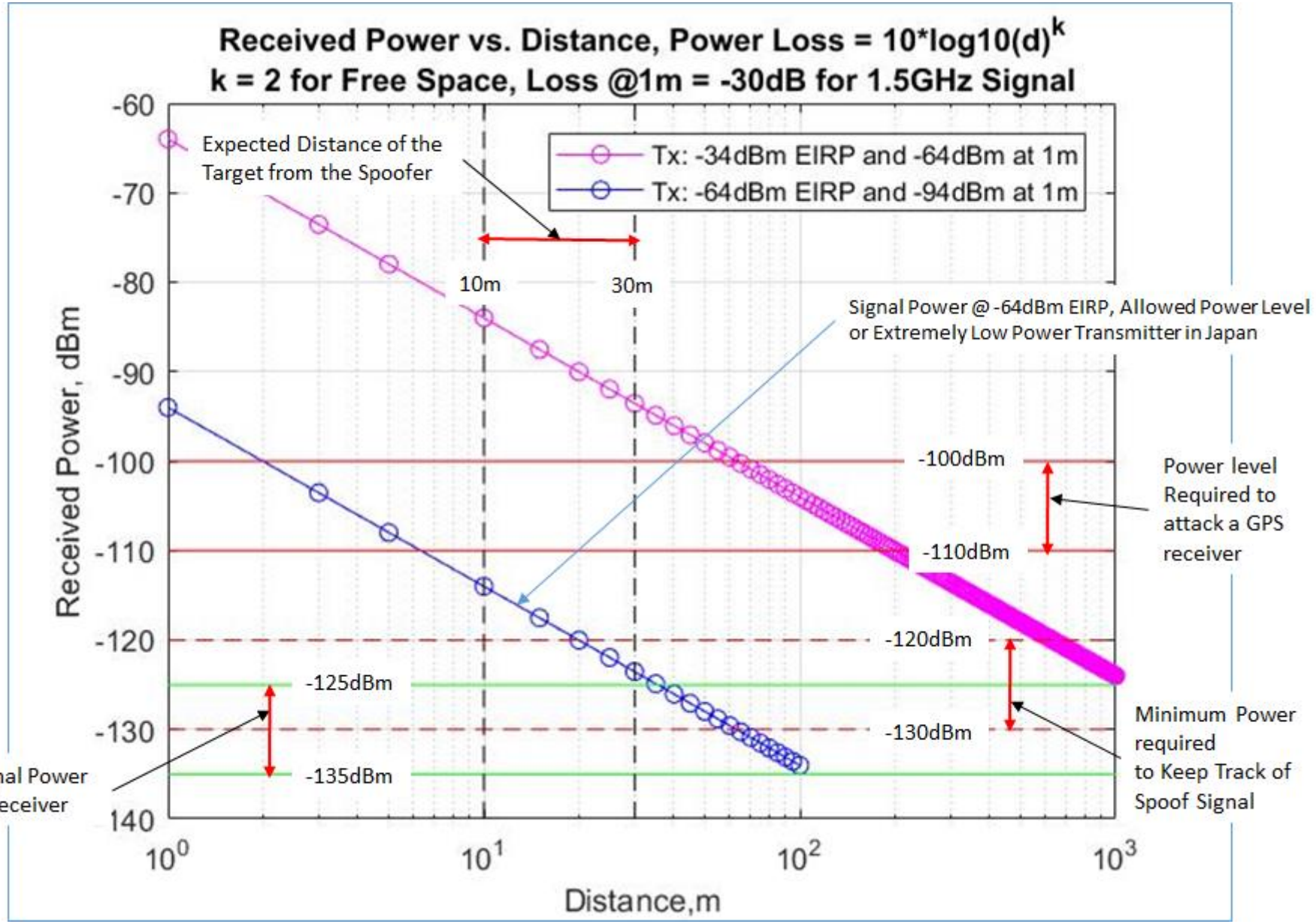
- **Allocation**
  - **Frequency separation of stations of different services**
- **Regulatory Protection**
  - **Not to cause harmful interference or claim protection**
- **Power Limits**
  - **PFD to protect Terrestrial services**
  - **EIRP to protect Space services**
  - **EPFD to protect GSO from NGSO**
- **Coordination**
  - **Between administrations to ensure interference-free operations conditions**

Source: Hon Fai Ng, RNSS & ITU Radio Regulations, ITU, 11th ICG Meeting, 2016, Sochi

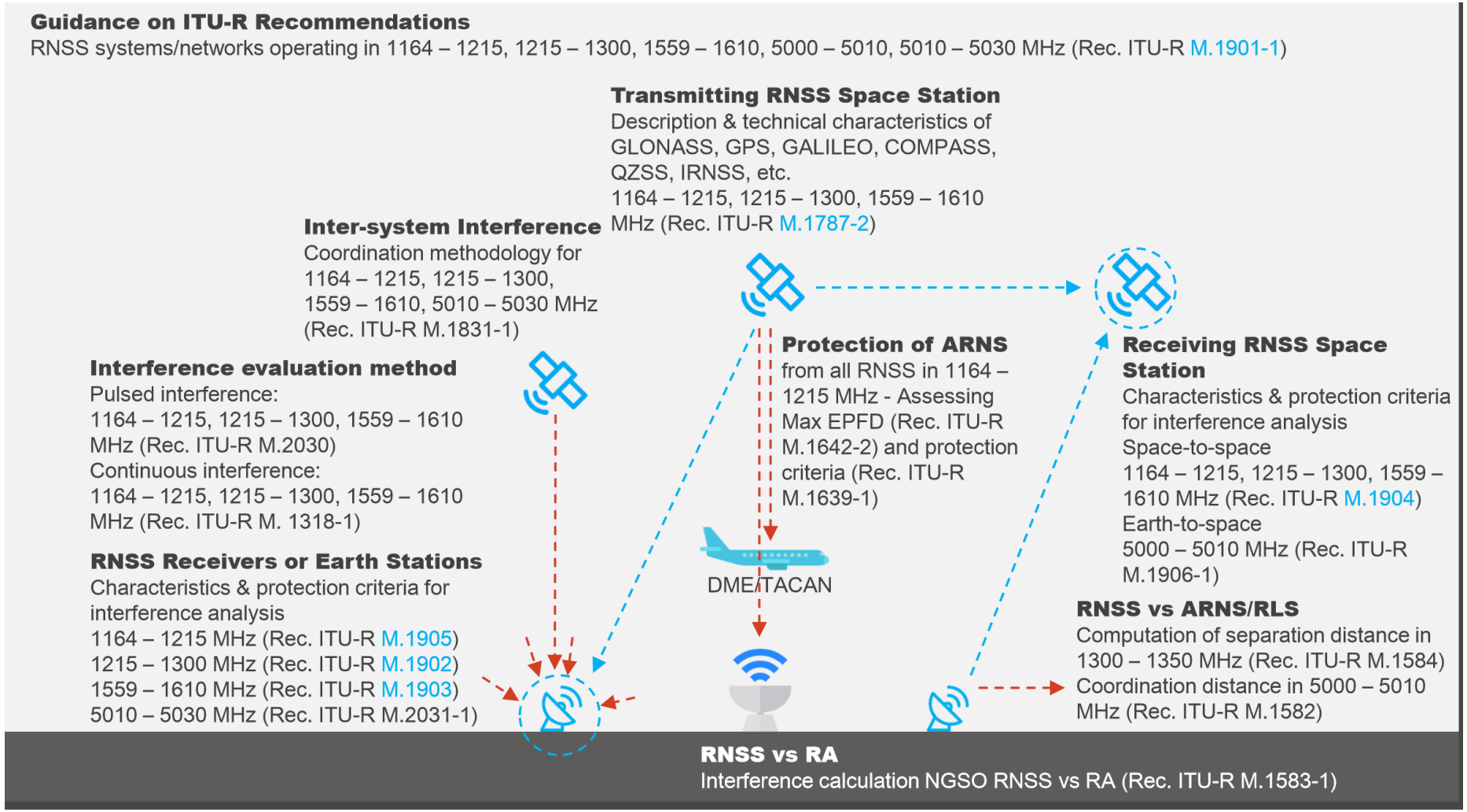
Maximum Field Intensity at 3m Distance from Antenna for Operation of License Free Weak Signals in Japan



Maximum Field Intensity of RF signal at 3m for License Free operation in Japan
For GPS , it is 35micro-volt/m at 3m from antenna. This corresponds to about -64dBm EIRP at antenna

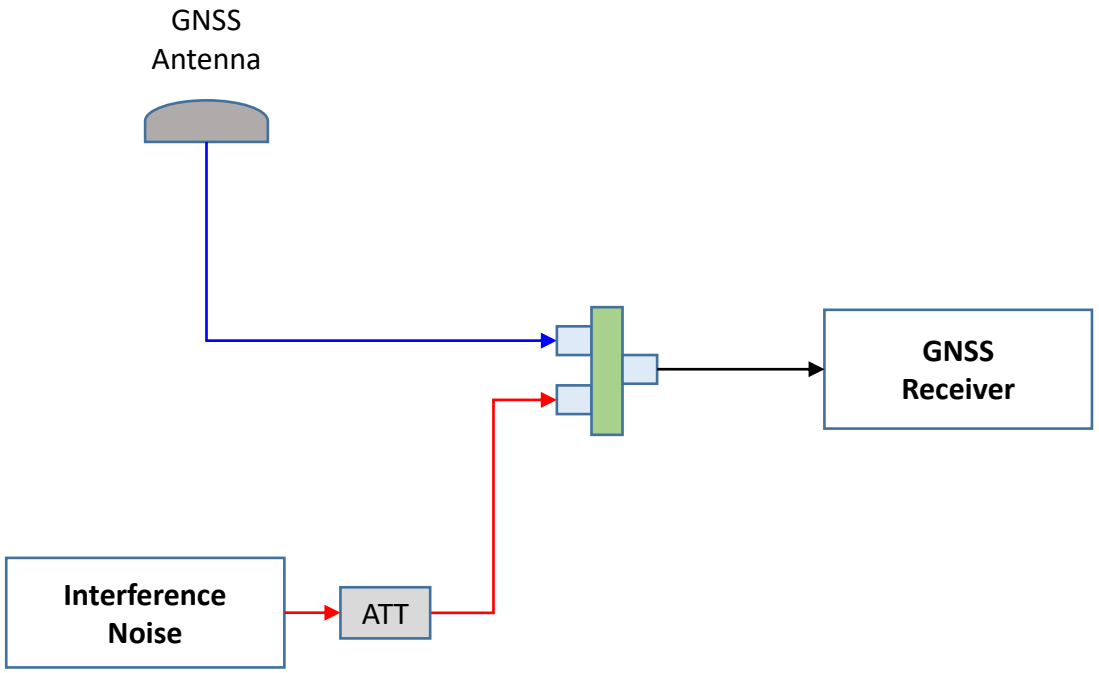

Received Power vs. Distance, Power Loss = 10*log10(d)^k
k = 2 for Free Space, Loss @1m = -30dB for 1.5GHz Signal
Expected Distance of the Target from the Spoofer
Tx: -34dBm EIRP and -64dBm at 1m
Tx: -64dBm EIRP and -94dBm at 1m
10m
30m
Signal Power @ -64dBm EIRP, Allowed Power Level or Extremely Low Power Transmitter in Japan
-100dBm
-110dBm
Power level Required to attack a GPS receiver
-120dBm
-125dBm
-130dBm
-135dBm
GPS Signal Power at the Receiver
Minimum Power required to Keep Track of Spoof Signal
Received Power, dBm
Distance,m
-60
-70
-80
-90
-100
-110
-120
-130
140
10^0
10^1
10^2
10^3

ITU RNSS Documents



Please refer ITU documents for details on regulations related with GNSS signals

GNSS Signal with Interference Noise IF Data Samples



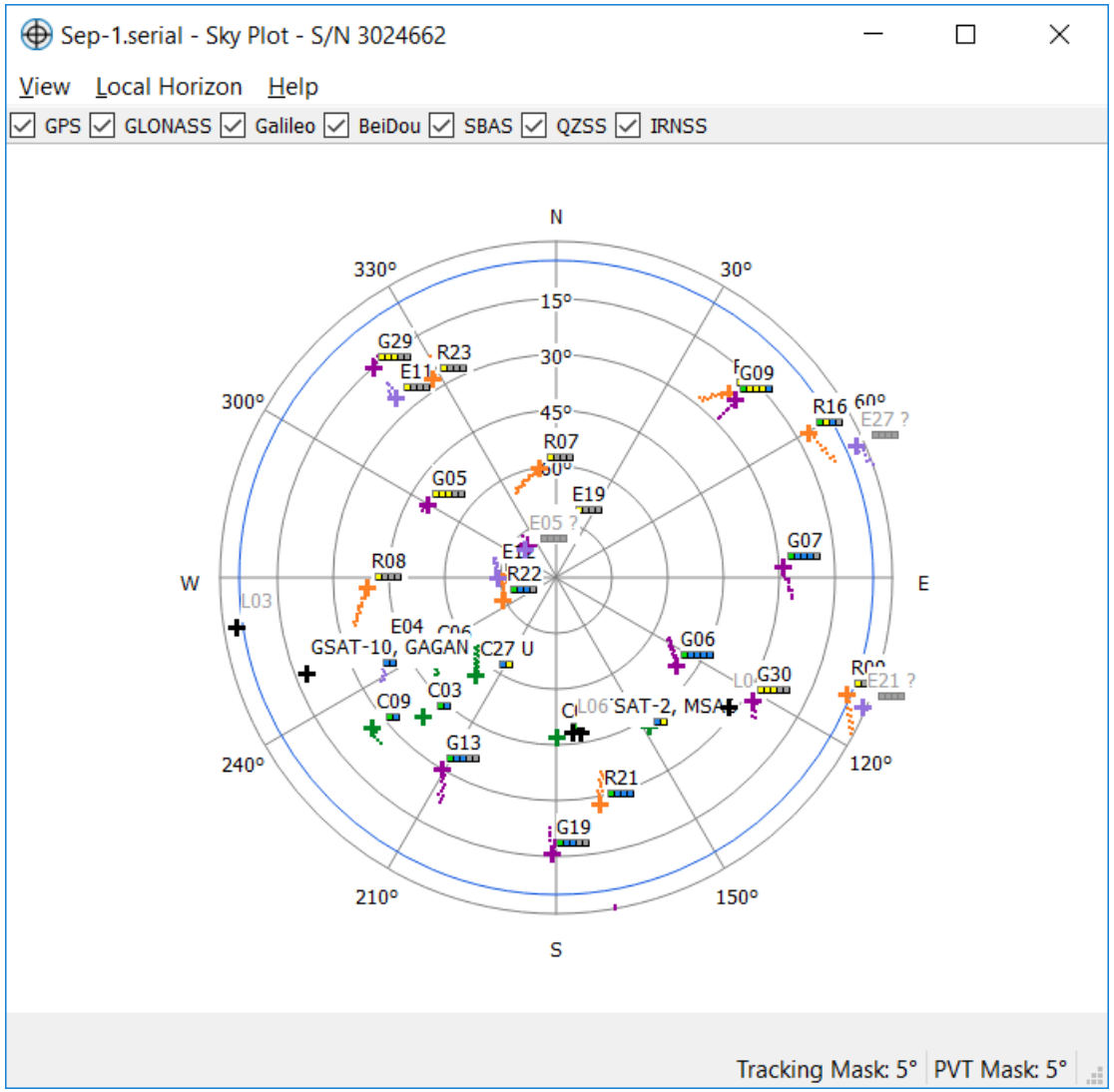
AGC and Sky Plot
Normal GNSS Signal, No Interference Signal Present

	T1	T2
Source	Antenna	Interference Signal
IF Frequency	1584	Not Present
Int. ATT		
Ext. ATT		
System	GNSS	
Signal Type	Multi GNSS L1 L2, L5	

Sep-1.serial - AGC Table - S/N 3024662

View Help

	Front End 0	Front End 1	Front End 2	Front End 3	Front End 4	Front End 5	Front End 6
Front End Code	GPSL1/E1	GLOL1	B1	L5/E5a	E5b/B2	GPSL2	GLOL2
Antenna	MAIN	MAIN	MAIN	MAIN	MAIN	MAIN	MAIN
Gain (dB)	47	51	49	43	42	41	42
Sample Variance	89	98	96	100	96	104	102
Blanking (%)	0	0	0	0	0	0	0

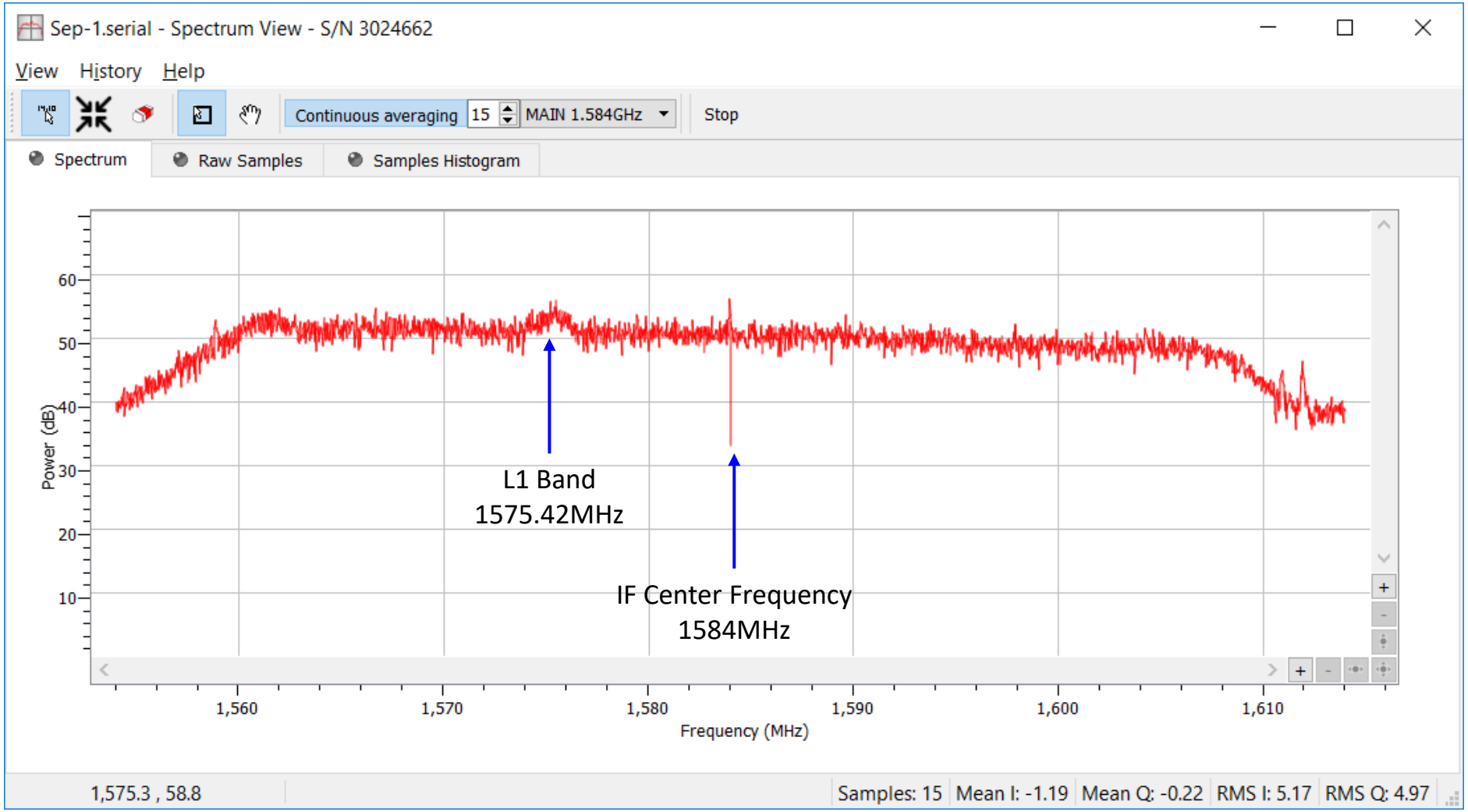


Raw Sample IF Signal, Center Frequency: 1584MHz
Normal GNSS Signal, No Interference Signal Present

	T1	T2
Source	Antenna	Interference Signal
IF Frequency	1584	Not Present
Int. ATT		
Ext. ATT		
System	GNSS	
Signal Type	Multi GNSS L1 L2, L5	

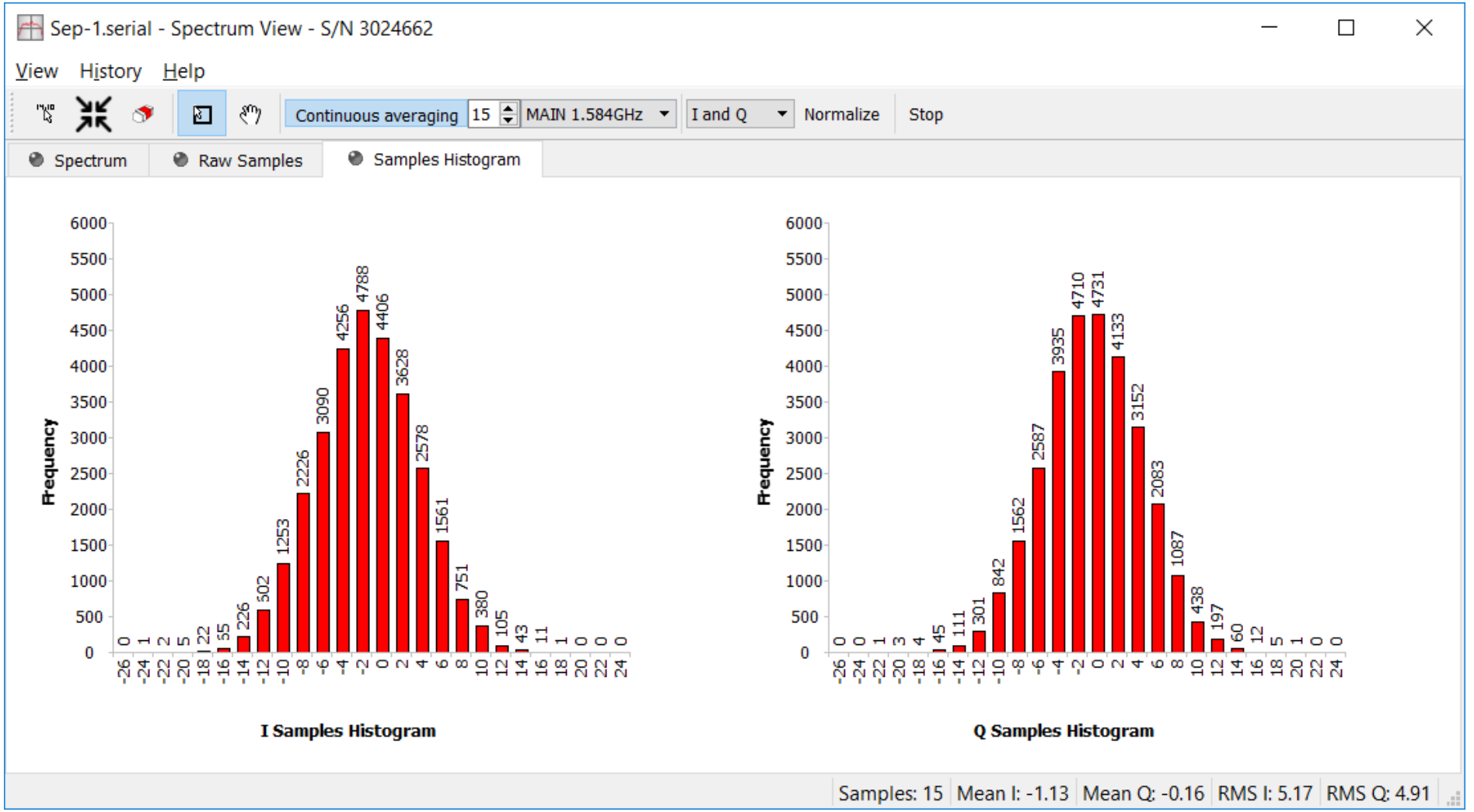
Power Spectrum of IF Signal, Center Frequency: 1584MHz
Normal GNSS Signal, No Interference Signal Present

	T1	T2
Source	Antenna	Interference Signal
IF Frequency	1584	Not Present
Int. ATT		
Ext. ATT		
System	GNSS	
Signal Type	Multi GNSS L1 L2, L5	



Histogram of IF Signal, Center Frequency: 1584MHz Normal GNSS Signal, No Interference Signal Present

	T1	T2
Source	Antenna	Interference Signal
IF Frequency	1584	Not Present
Int. ATT		
Ext. ATT		
System	GNSS	
Signal Type	Multi GNSS L1 L2, L5	



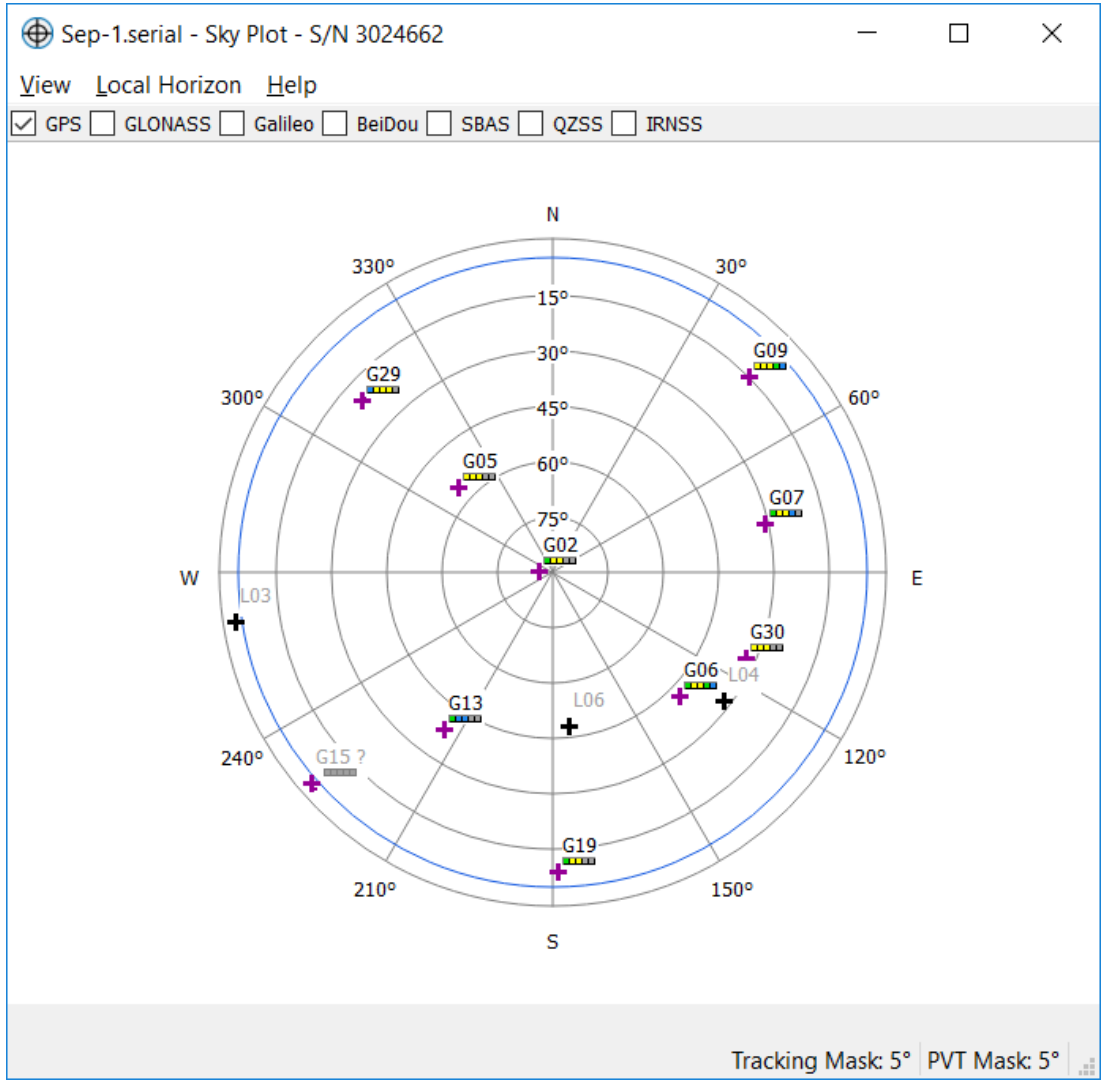
AGC and Sky Plot
Normal GNSS Signal and Interference Signal

	T1	T2
Source	Antenna	Interference Signal
IF Frequency	1584	1575.42
Int. ATT		10
Ext. ATT		30
System	GNSS	GPS
Signal Type	Multi GNSS L1 L2, L5	L1 Only

Sep-1.serial - AGC Table - S/N 3024662

View Help

	Front End 0	Front End 1	Front End 2	Front End 3	Front End 4	Front End 5	Front End 6
Front End Code	GPSL1/E1	GLOL1	B1	L5/E5a	E5b/B2	GPSL2	GLOL2
Antenna	MAIN	MAIN	MAIN	MAIN	MAIN	MAIN	MAIN
Gain (dB)	44	50	47	41	41	39	41
Sample Variance	100	98	102	100	100	93	98
Blanking (%)	0	0	0	0	0	0	0

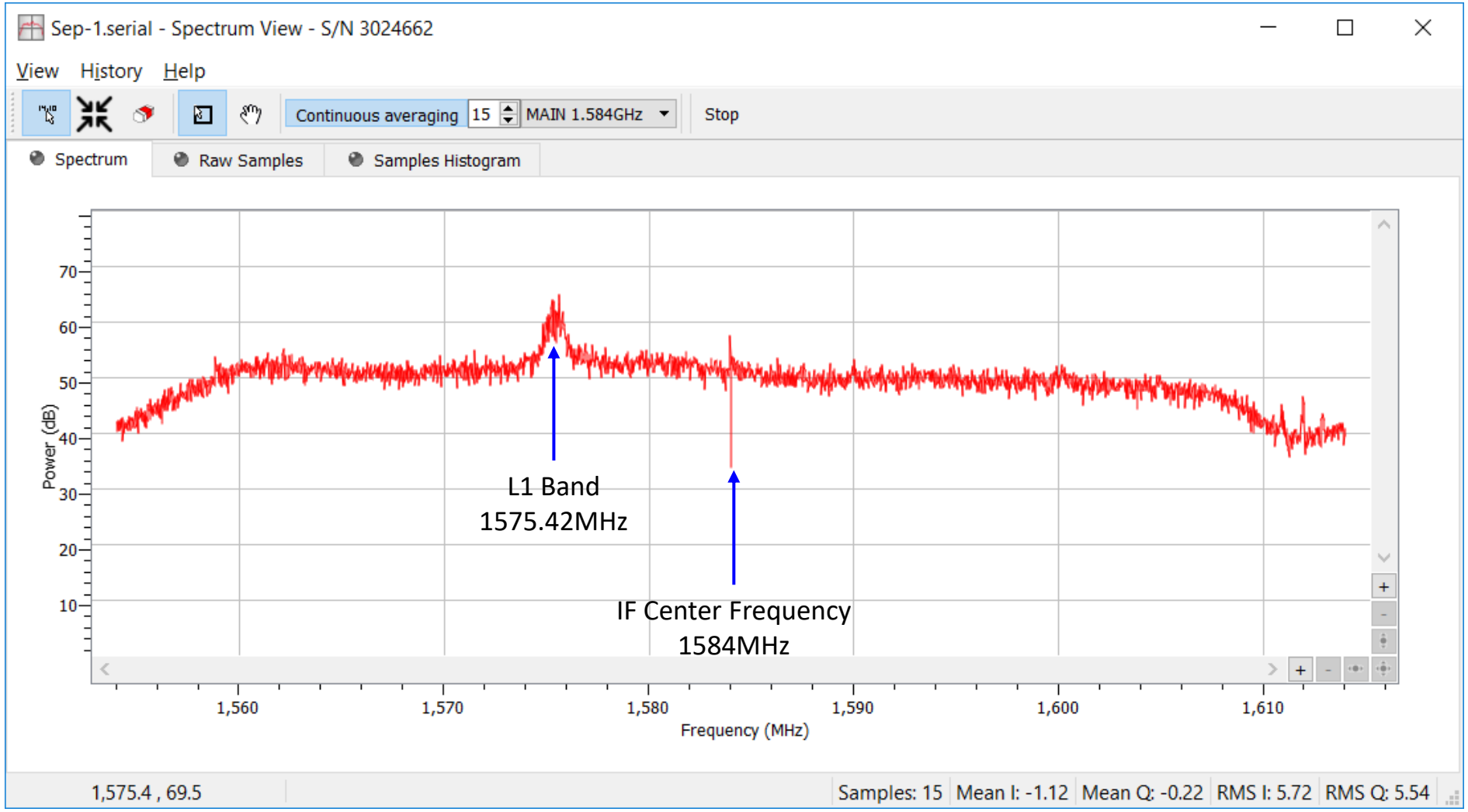


Raw Sample IF Signal, Center Frequency: 1584MHz
Normal GNSS Signal and Interference Signal

	T1	T2
Source	Antenna	Interference Signal
IF Frequency	1584	1575.42
Int. ATT		10
Ext. ATT		30
System	GNSS	GPS
Signal Type	Multi GNSS L1 L2, L5	L1 Only

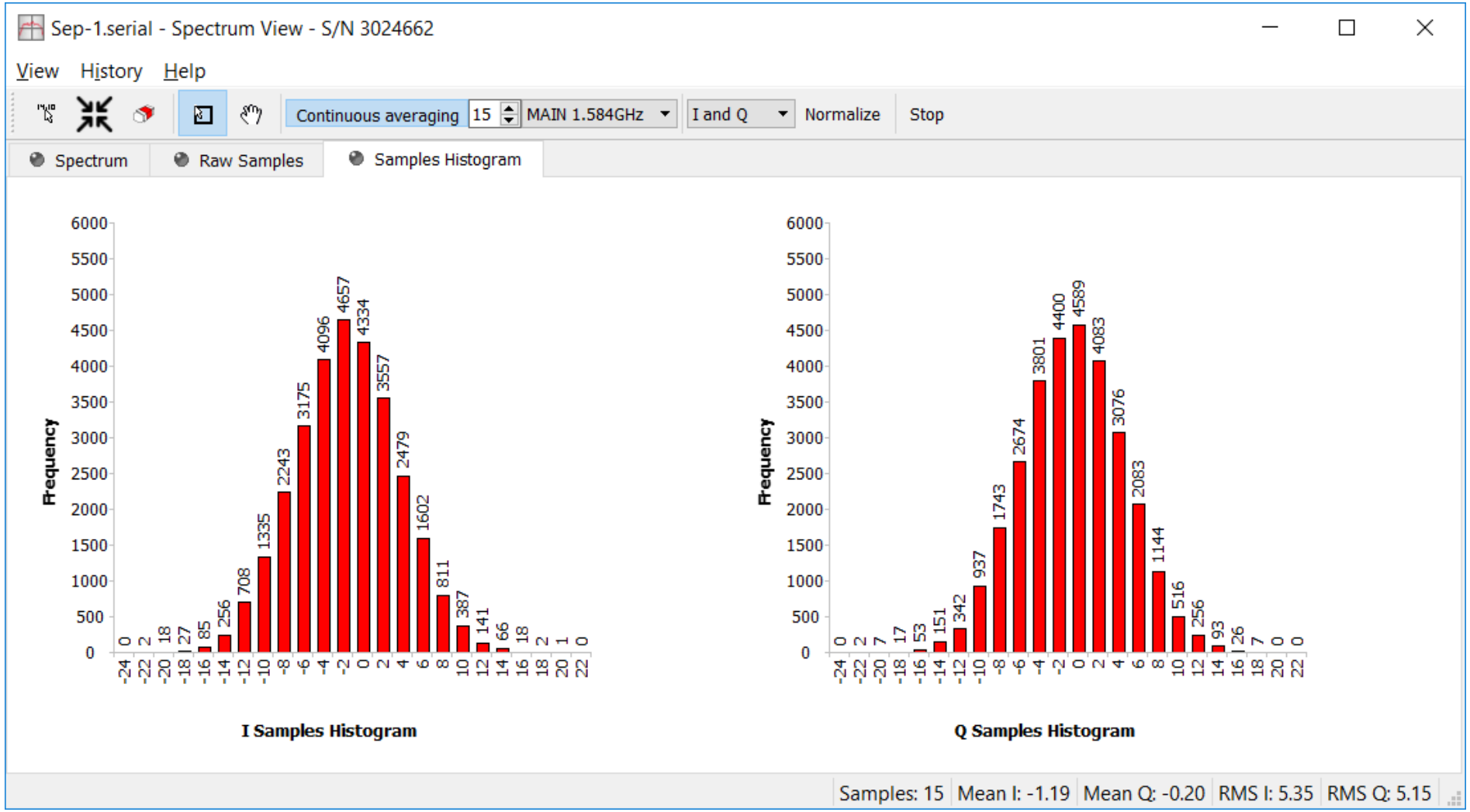
Power Spectrum of IF Signal, Center Frequency: 1584MHz
Normal GNSS Signal and Interference Signal

	T1	T2
Source	Antenna	Interference Signal
IF Frequency	1584	1575.42
Int. ATT		10
Ext. ATT		30
System	GNSS	GPS
Signal Type	Multi GNSS L1 L2, L5	L1 Only



Histogram of IF Signal, Center Frequency: 1584MHz
Normal GNSS Signal and Interference Signal

	T1	T2
Source	Antenna	Interference Signal
IF Frequency	1584	1575.42
Int. ATT		10
Ext. ATT		30
System	GNSS	GPS
Signal Type	Multi GNSS L1 L2, L5	L1 Only



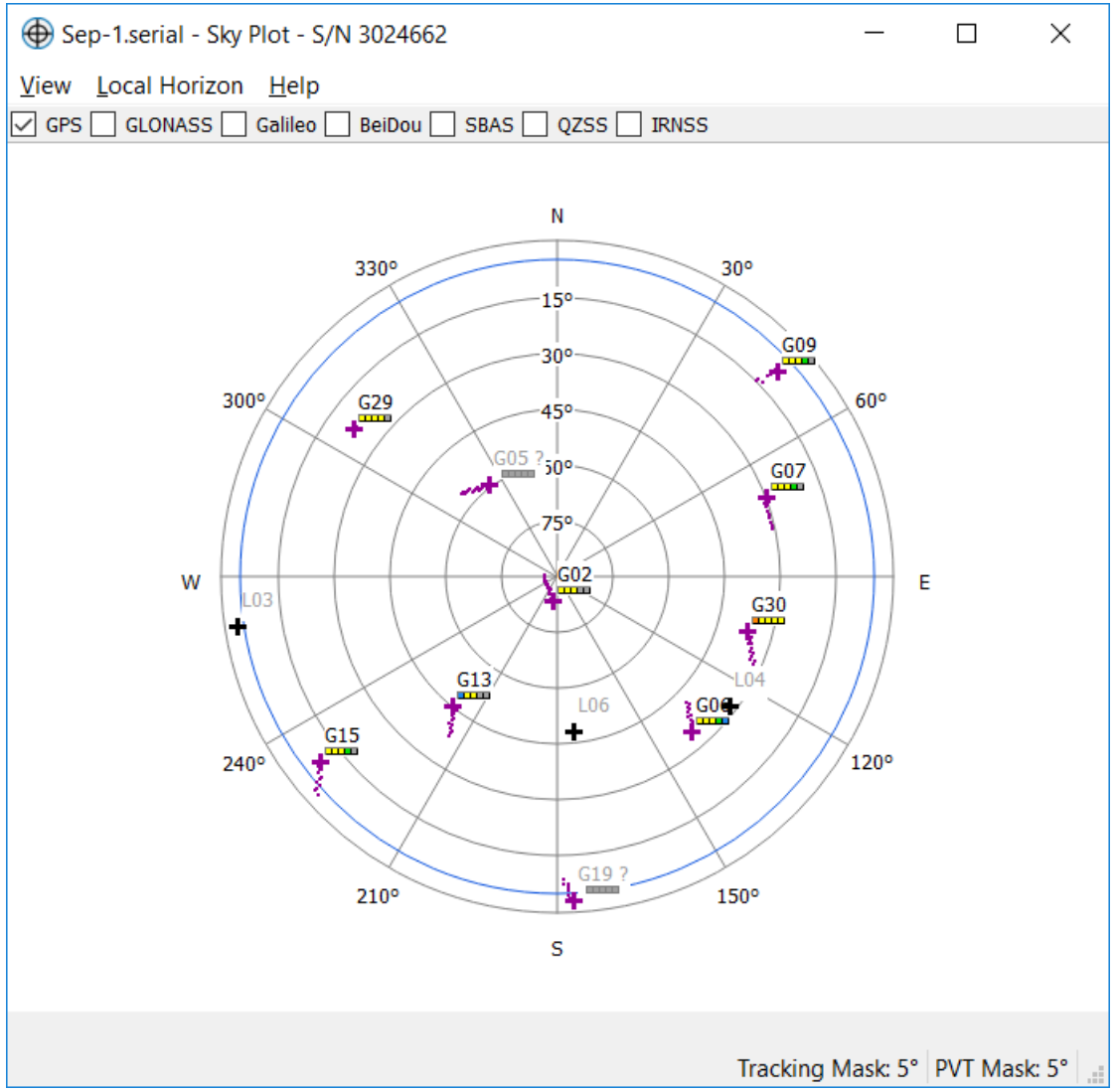
AGC and Sky Plot
Normal GNSS Signal and Strong Interference Signal

	T1	T2
Source	Antenna	Interference Signal
IF Frequency	1584	1575.42
Int. ATT		10
Ext. ATT		10
System	GNSS	GPS
Signal Type	Multi GNSS L1 L2, L5	L1 Only

Sep-1.serial - AGC Table - S/N 3024662

View Help

	Front End 0	Front End 1	Front End 2	Front End 3	Front End 4	Front End 5	Front End 6
Front End Code	GPSL1/E1	GLOL1	B1	L5/E5a	E5b/B2	GPSL2	GLOL2
Antenna	MAIN	MAIN	MAIN	MAIN	MAIN	MAIN	MAIN
Gain (dB)	23	49	28	40	40	39	41
Sample Variance	100	102	104	100	93	96	100
Blanking (%)	0	0	0	0	0	0	0

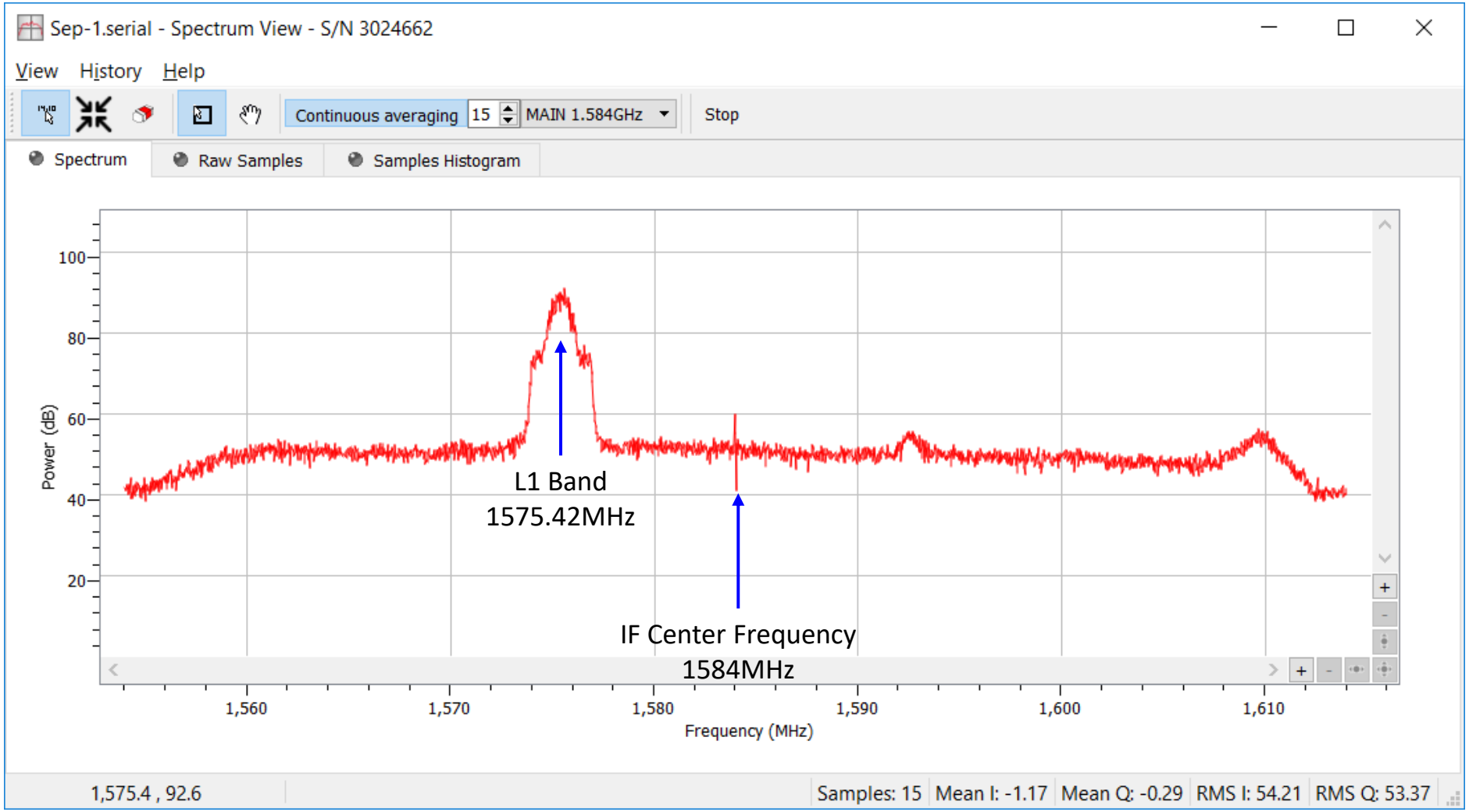


Raw Sample IF Signal, Center Frequency: 1584MHz Normal GNSS Signal and Strong Interference Signal

	T1	T2
Source	Antenna	Interference Signal
IF Frequency	1584	1575.42
Int. ATT		10
Ext. ATT		10
System	GNSS	GPS
Signal Type	Multi GNSS L1 L2, L5	L1 Only

Power Spectrum of IF Signal, Center Frequency: 1584MHz Normal GNSS Signal and Strong Interference Signal

	T1	T2
Source	Antenna	Interference Signal
IF Frequency	1584	1575.42
Int. ATT		10
Ext. ATT		10
System	GNSS	GPS
Signal Type	Multi GNSS L1 L2, L5	L1 Only



Histogram of IF Signal, Center Frequency: 1584MHz Normal GNSS Signal and Strong Interference Signal

	T1	T2
Source	Antenna	Interference Signal
IF Frequency	1584	1575.42
Int. ATT		10
Ext. ATT		10
System	GNSS	GPS
Signal Type	Multi GNSS L1 L2, L5	L1 Only