Facing the New Era of GNSS Hacking

Tomas Rosa, Raiffeisen BANK Cryptology and Biometrics Competence Centre

DAILY NEWS 10 August 2017

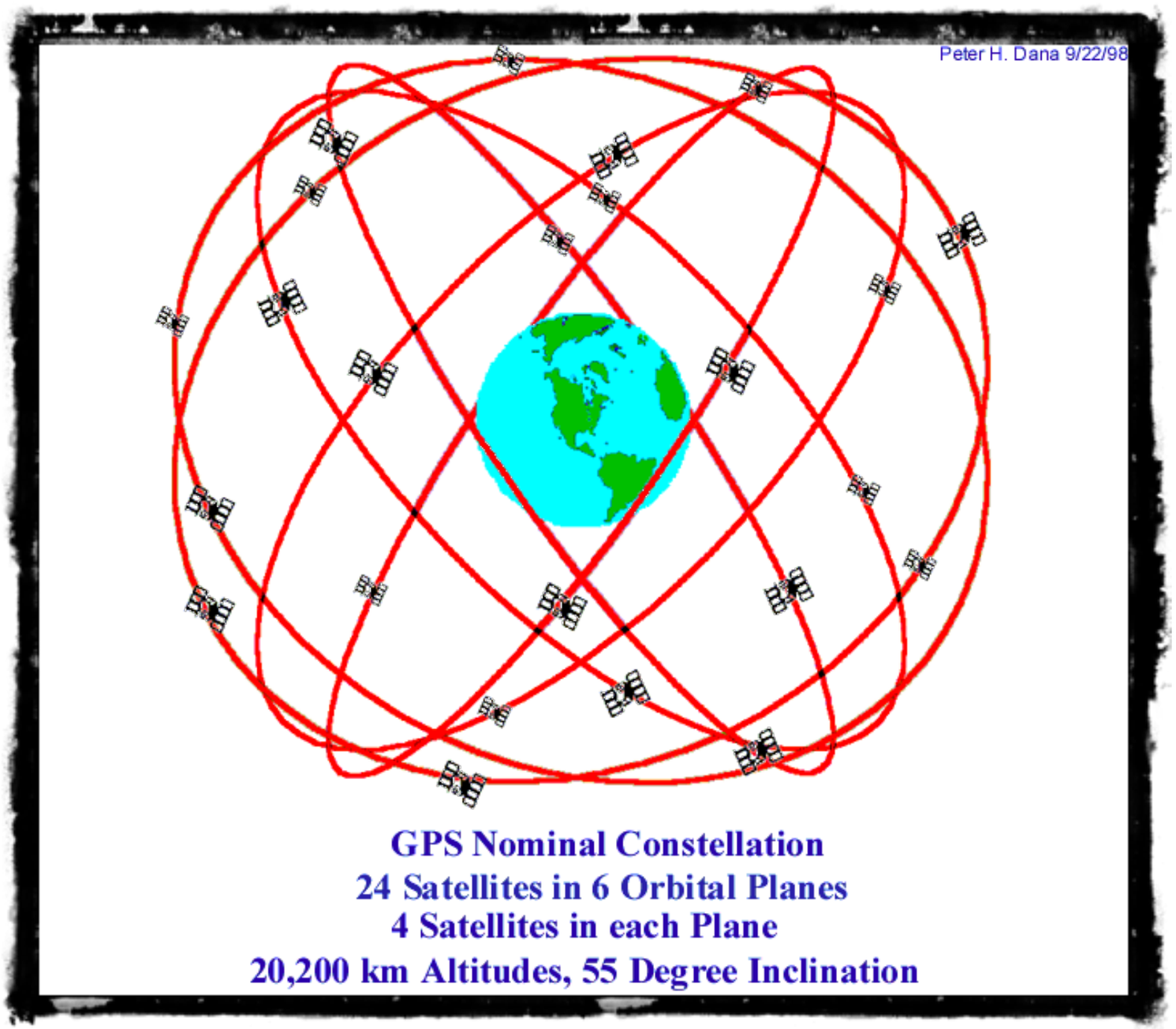
Ships fooled in GPS spoofing attack suggest Russian cyberweapon

Have you said *GNSS*?

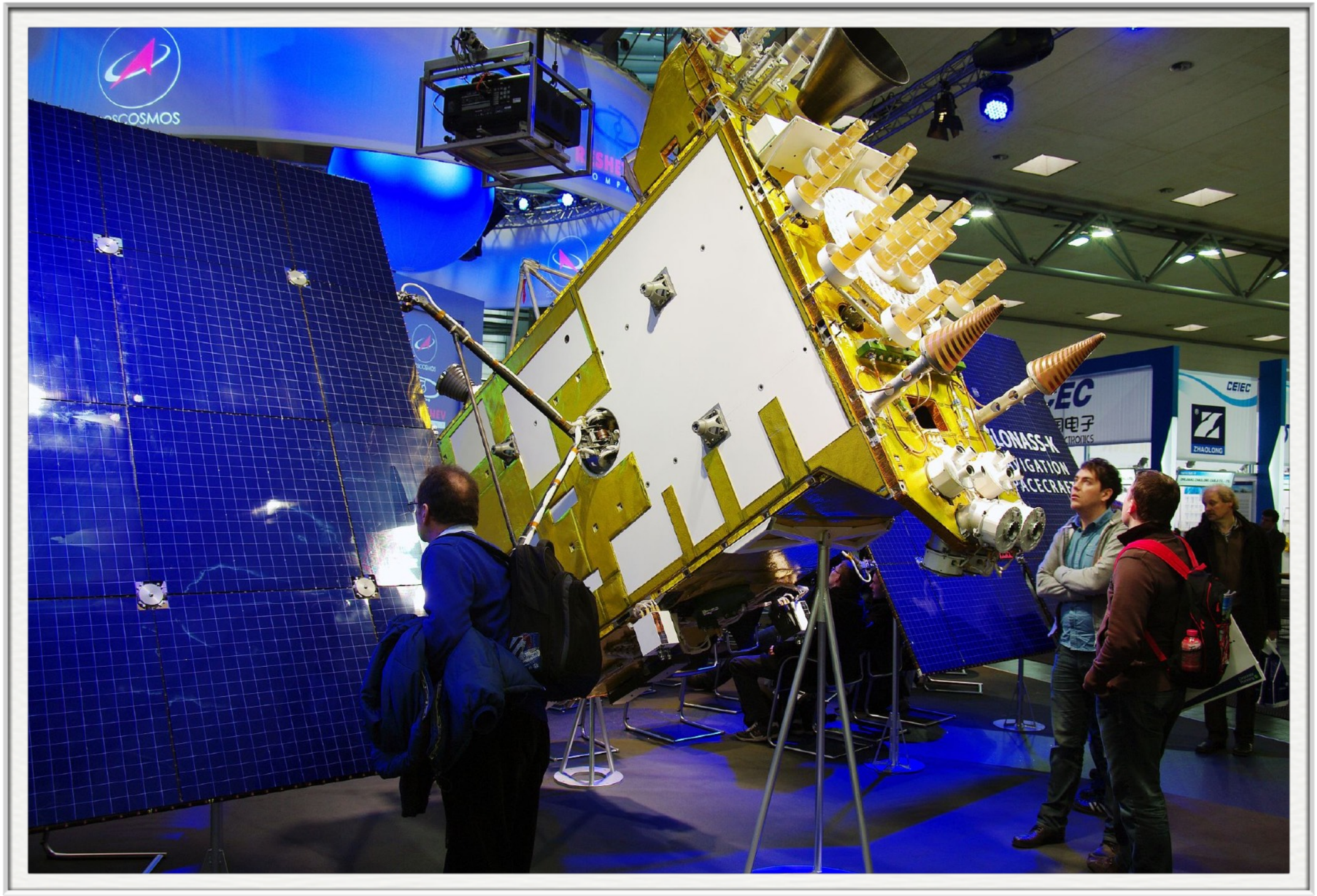
- GNSS stands for Global Navigation Satellite System(s)
- NAVSTAR GPS is one particular kind of GNSS
- The other ones are namely:
  - Chinese BeiDou-2 (former COMPASS)
  - European Galileo (governed by GSA in Prague)
  - Russian GLONASS (Globalnaya Navigatsionnaya Sputnikovaya Sistema)
- All of them are facing very similar problems with their civil services

GPS Space Segment Vehicle - SV - (Block IIF)

GPS Space Segment Constellation

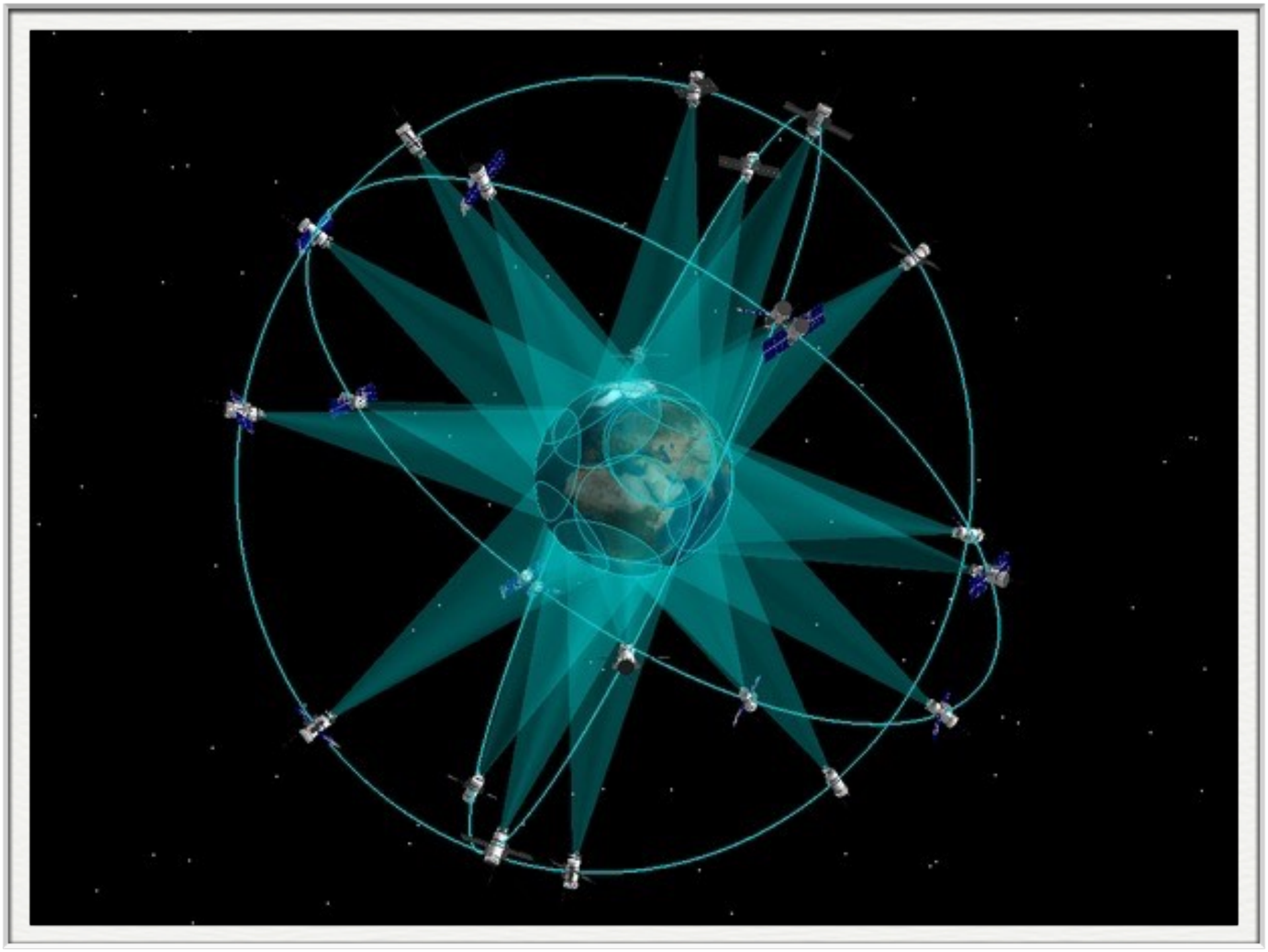


GLONASS Satellite K1 at CeBIT 2011



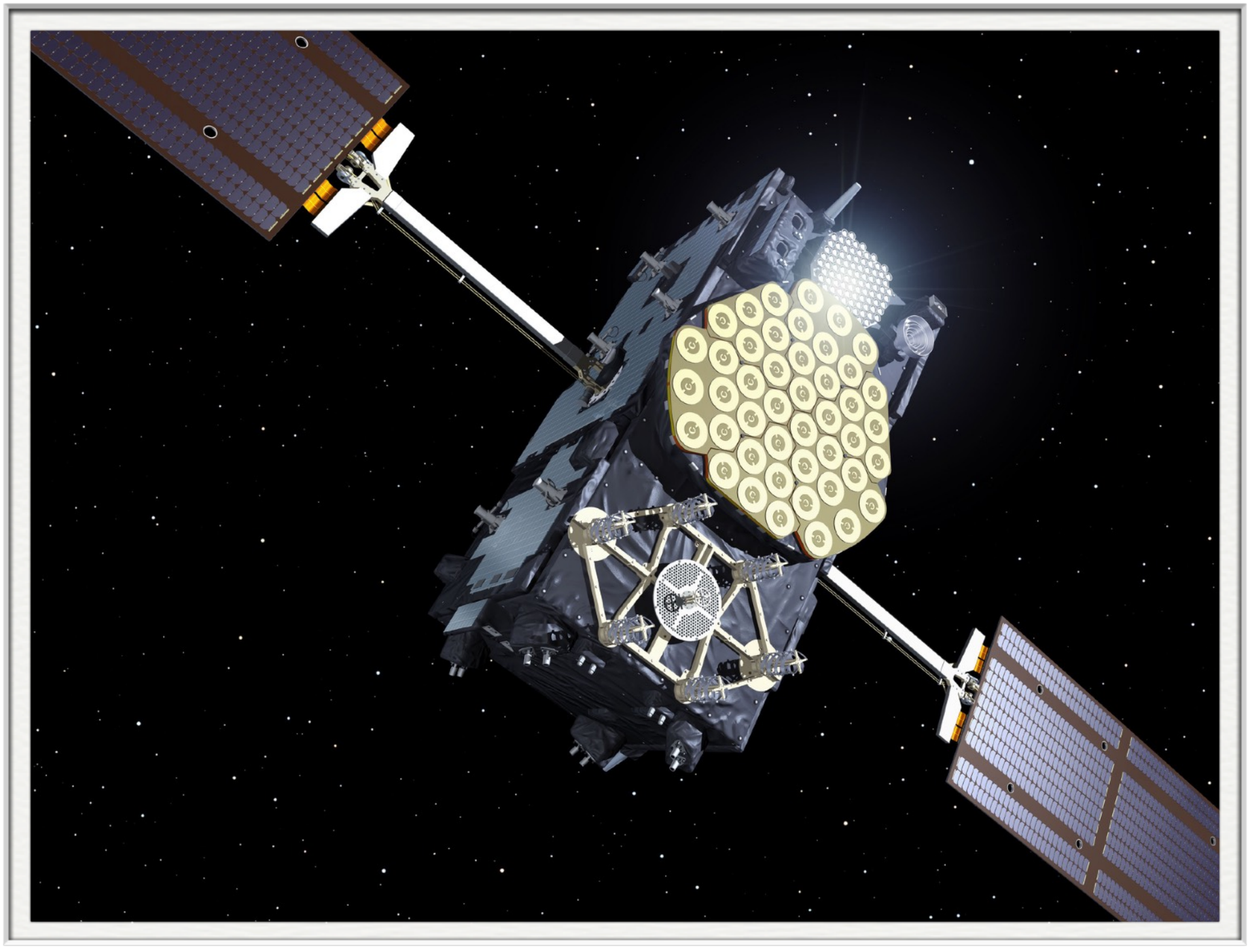
[foto by Jurgen Treutler]

GLONASS Constellation



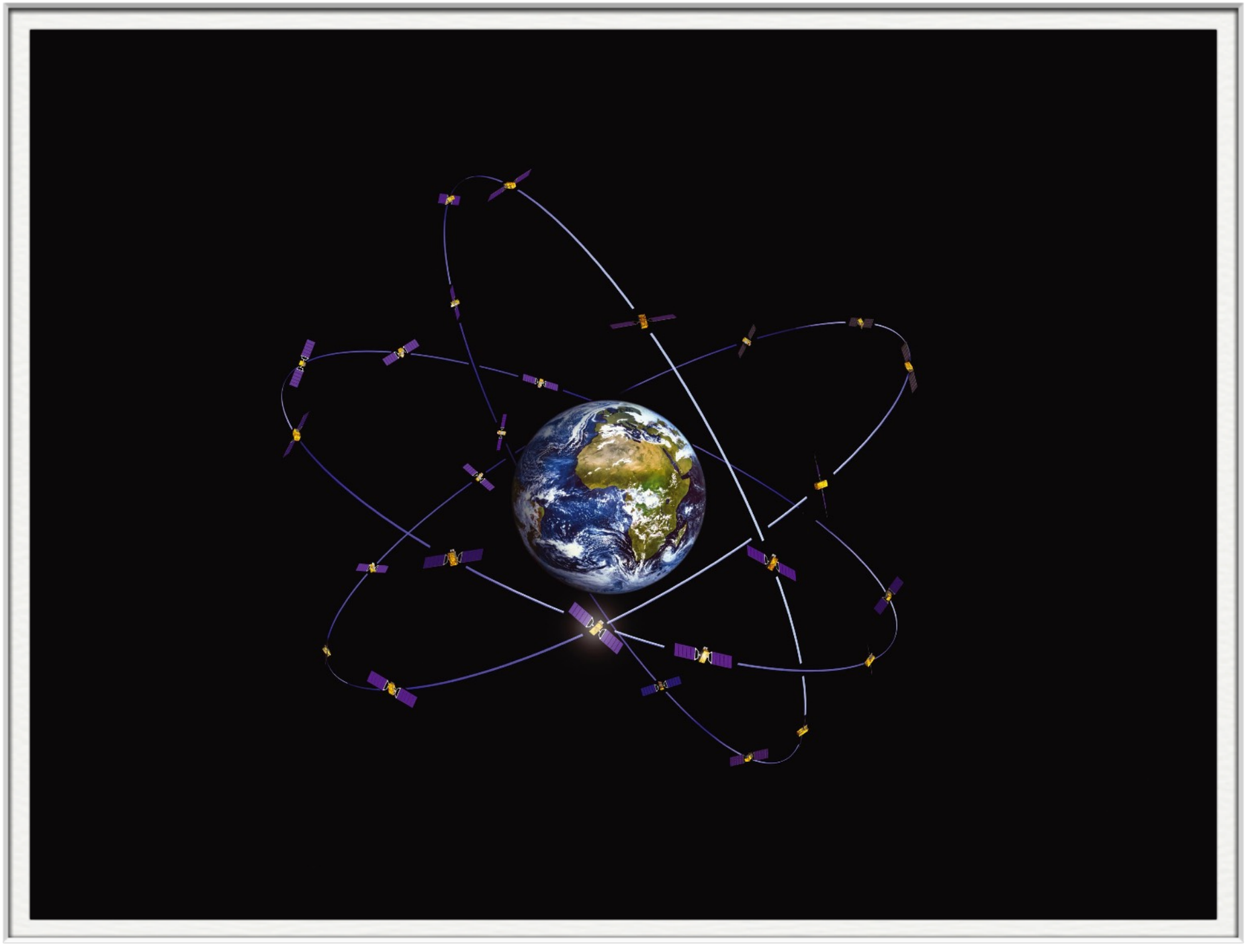
[Roscosmos]

Galileo Satellite (IOV Phase)



[European Astrotech]

Galileo Constellation



[European Space Agency]

Satellite clock observation expose time delay that in turn reveals the satellite distance

t_{sent_sv1}

t_{sent_sv2}

t_{sent_sv3}

four satellites to get X, Y, Z, and t_bias

$t_{rec}+t_{bias}$

t_{sent_sv4}

Satellite Clock Observation Revisited

- Let s_i denote the signal generated by SV_i, and let $\varphi(t)$ be any "reasonably" smooth function of time.

- Then one can recover $\varphi(t)$ by observing the received signal

$$s\_recv_i(t) = s_i(\varphi(t))$$

... this is achieved through implicit (carrier, chipping sequence, data modulation) and explicit (navigation data) time stamps embedded into the satellite signal

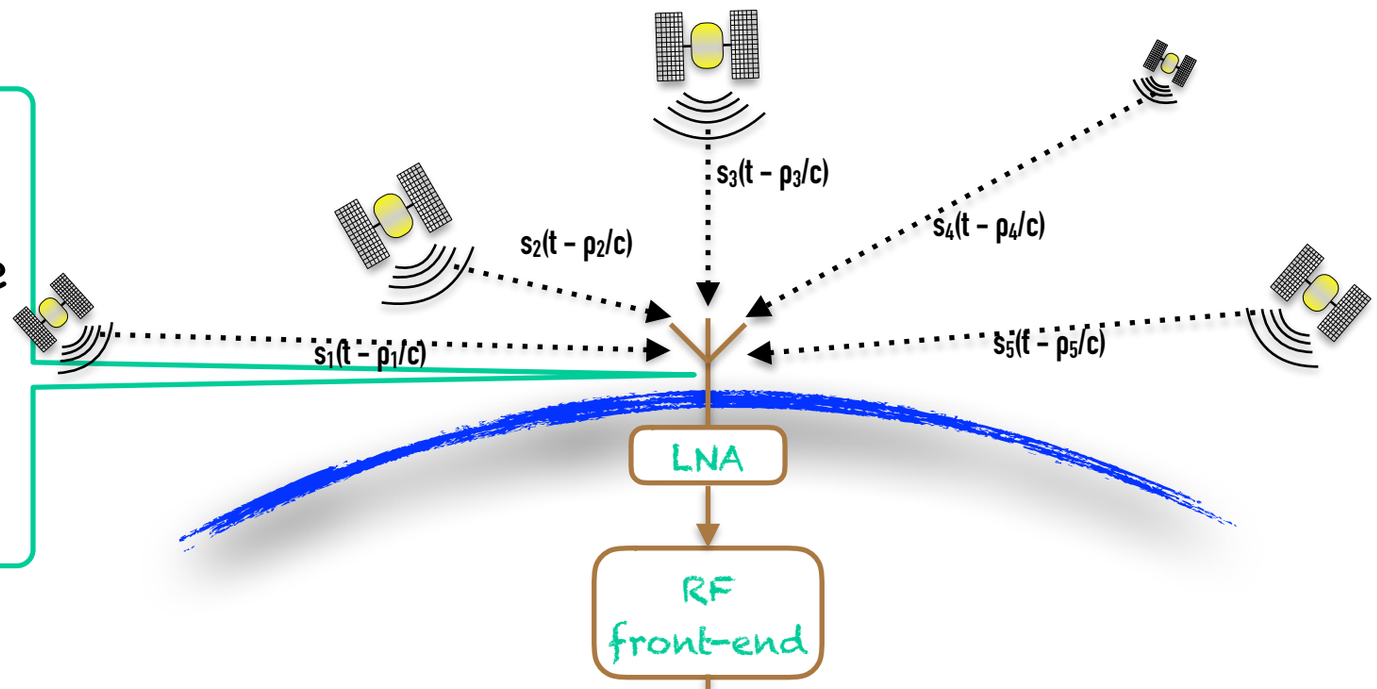
In first approximation, we let

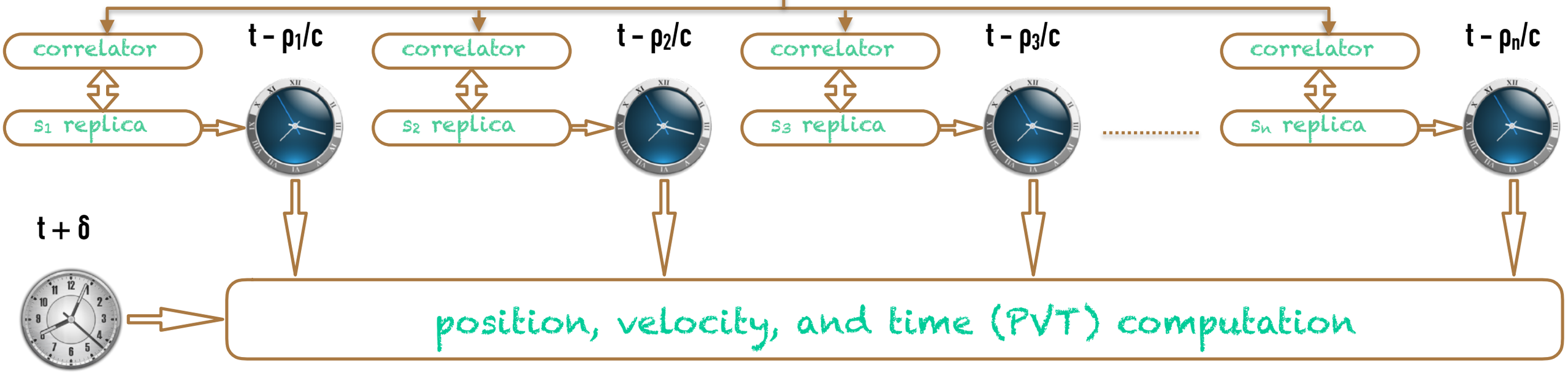
$$\varphi(t) = t - \frac{\rho_i}{c}$$

where ρ_i represents the distance travelled by the signal in between the observer and SV_i and t is the GPS master time, all in the observer's frame on Earth.

GNSS Tracking Illustration

Antenna phase center - apparent location of EM wave reception, according to which rho_i is considered.



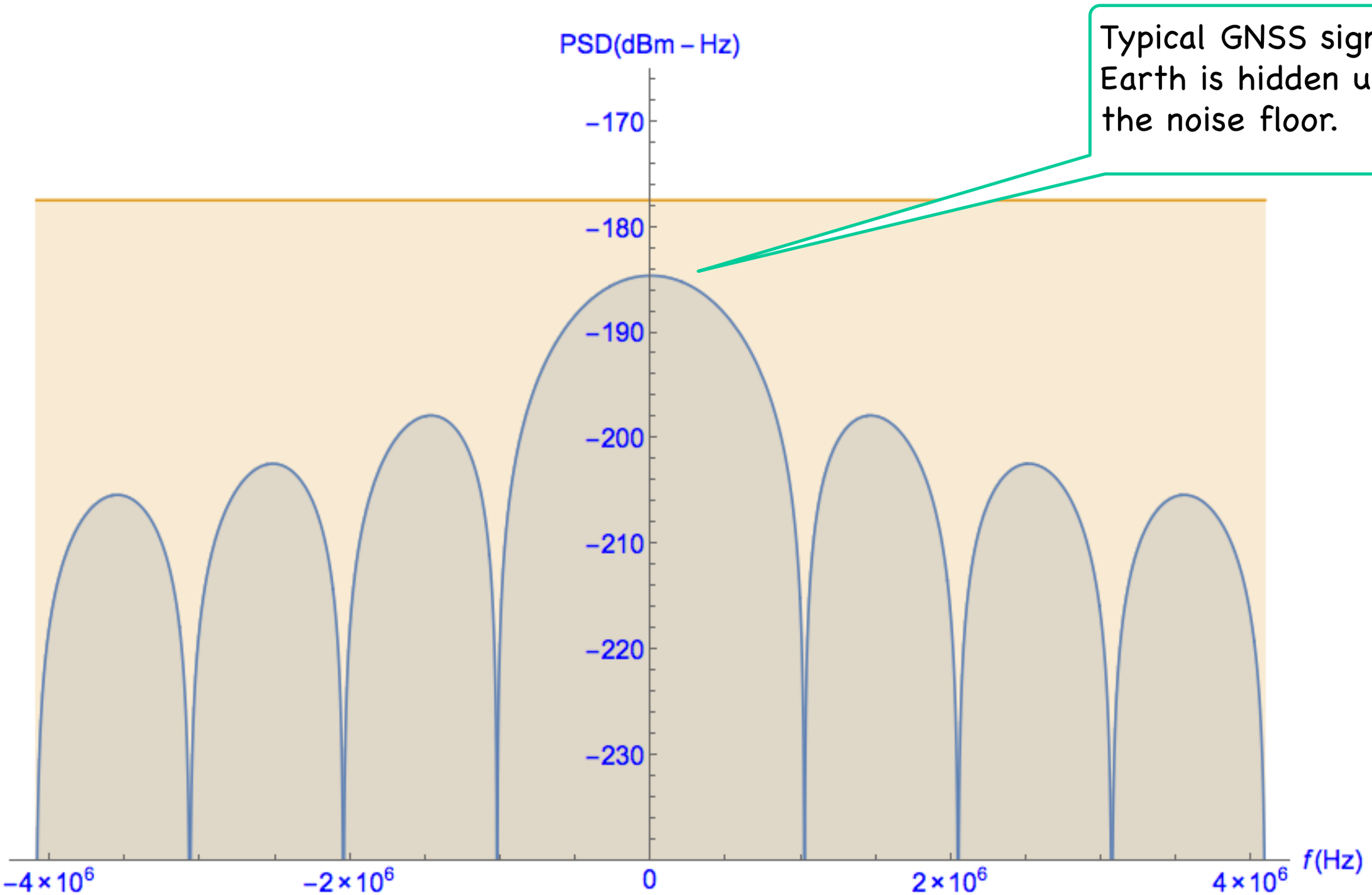


L1 C/A Signal in Detail

Carrier frequency	L1: 1575.42 MHz = 154 x 10.23 MHz
Minimum received power	-158.5 dBW = -128.5 dBm
Polarization	Right-Hand Circular Polarization (RHCP)
Multiple access	Code Division Multiple Access (CDMA)
Spreading modulation	Binary Phase-Shift Keying with Rectangular symbols and chipping rate 1 x 1.023 MHz ~ BPSK-R(1)
Tx bandwidth	±15.345 MHz; first null-to-null BW is 2.046 MHz
Spreading codes	Length 1023-bit Gold codes, duration 1 ms
Data message structure	NAV
Data rate	50 bps
Data error control code	Extended (32,26) Hamming code
Data modulation	50 sps biphase modulation
Pilot and data components	100% power data
Overlay code	None
Multiplexing with other signals	In phase quadrature to L1 P(Y), etc.

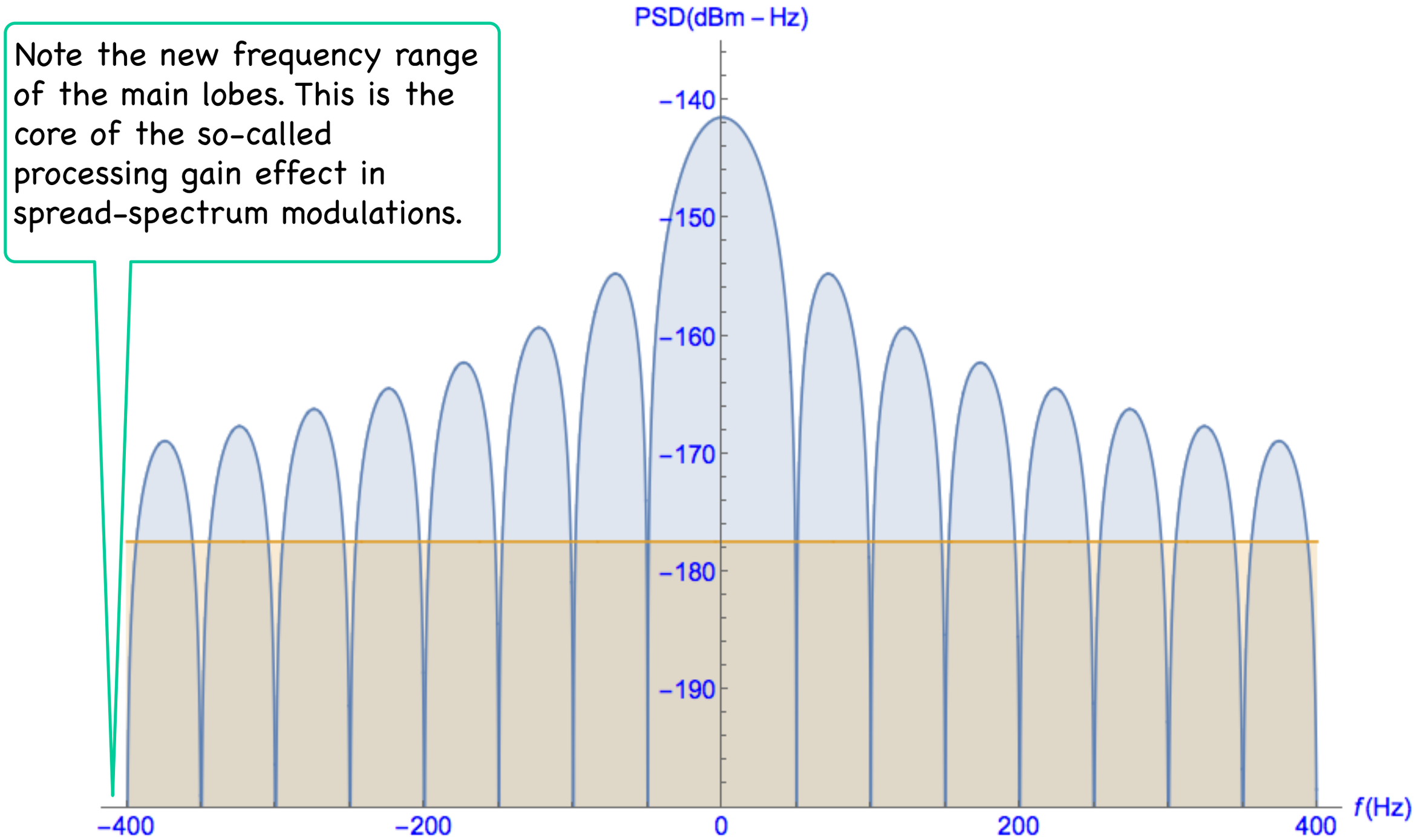
[Betz, 16]

L1 C/A Typical Antenna Received Signal Power Spectral Density Envelope vs. Background Noise Level (130 K)

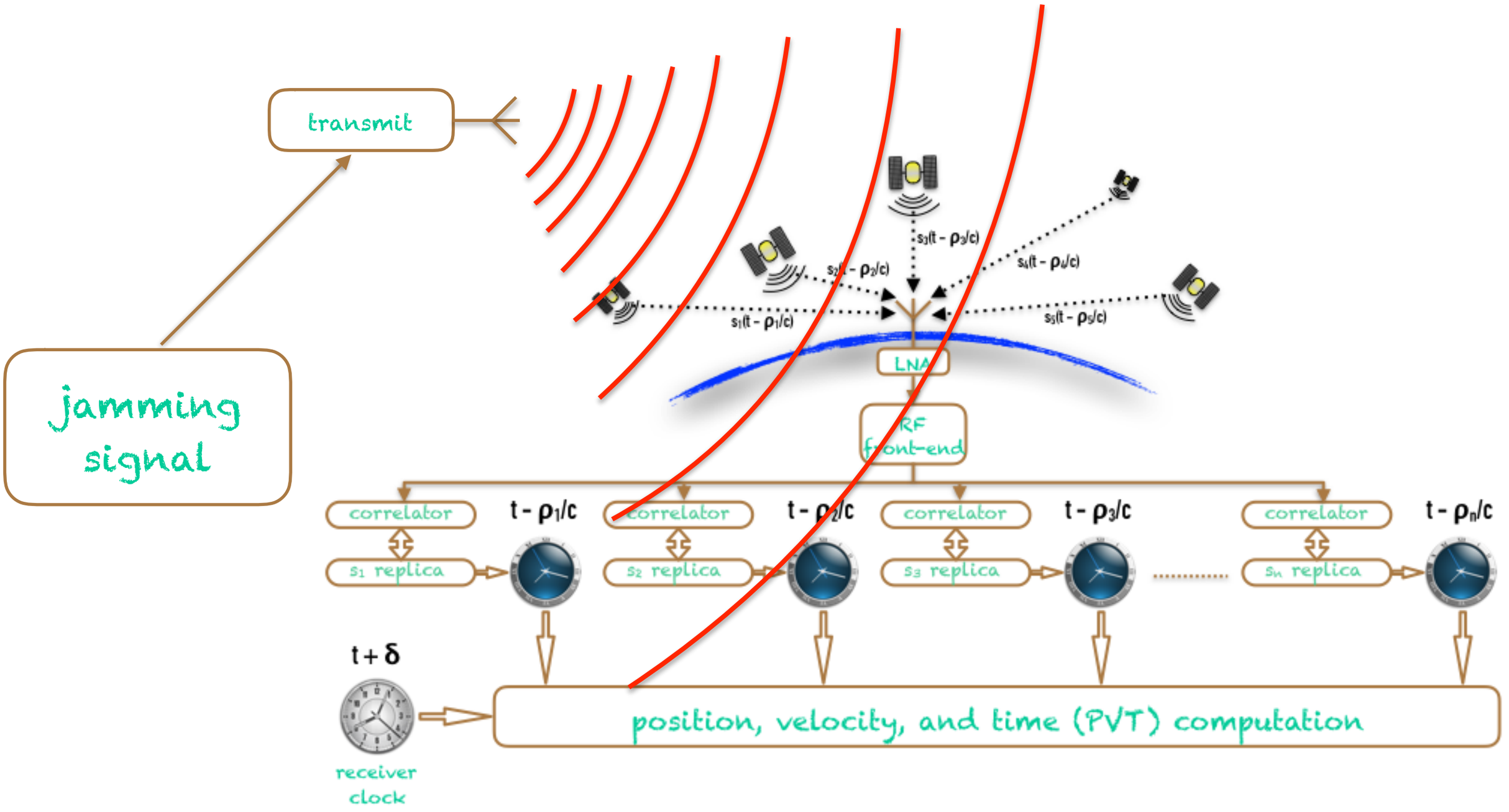


L1 C/A After Correlation-Based Despreading

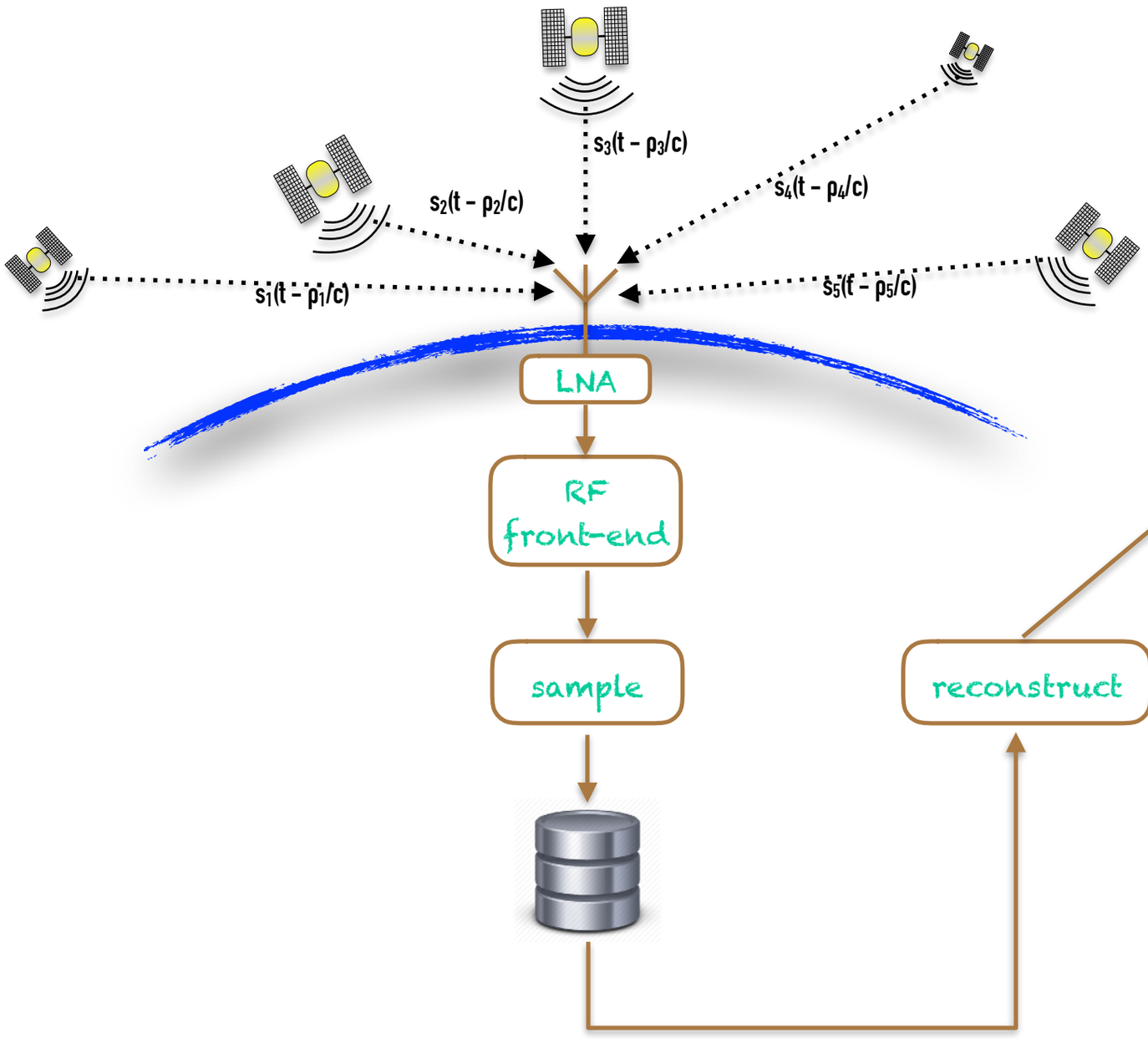
Note the new frequency range of the main lobes. This is the core of the so-called processing gain effect in spread-spectrum modulations.

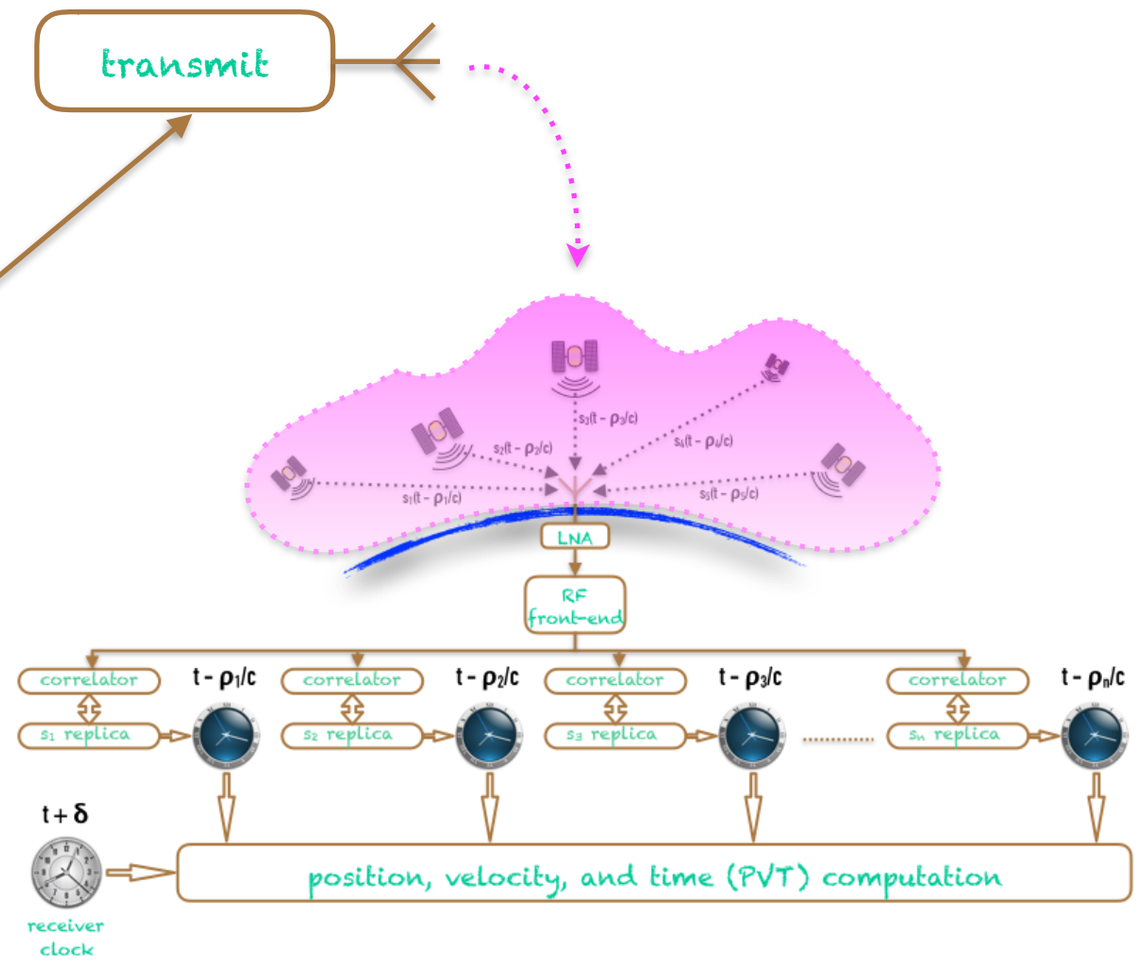


GNSS Jamming Attack

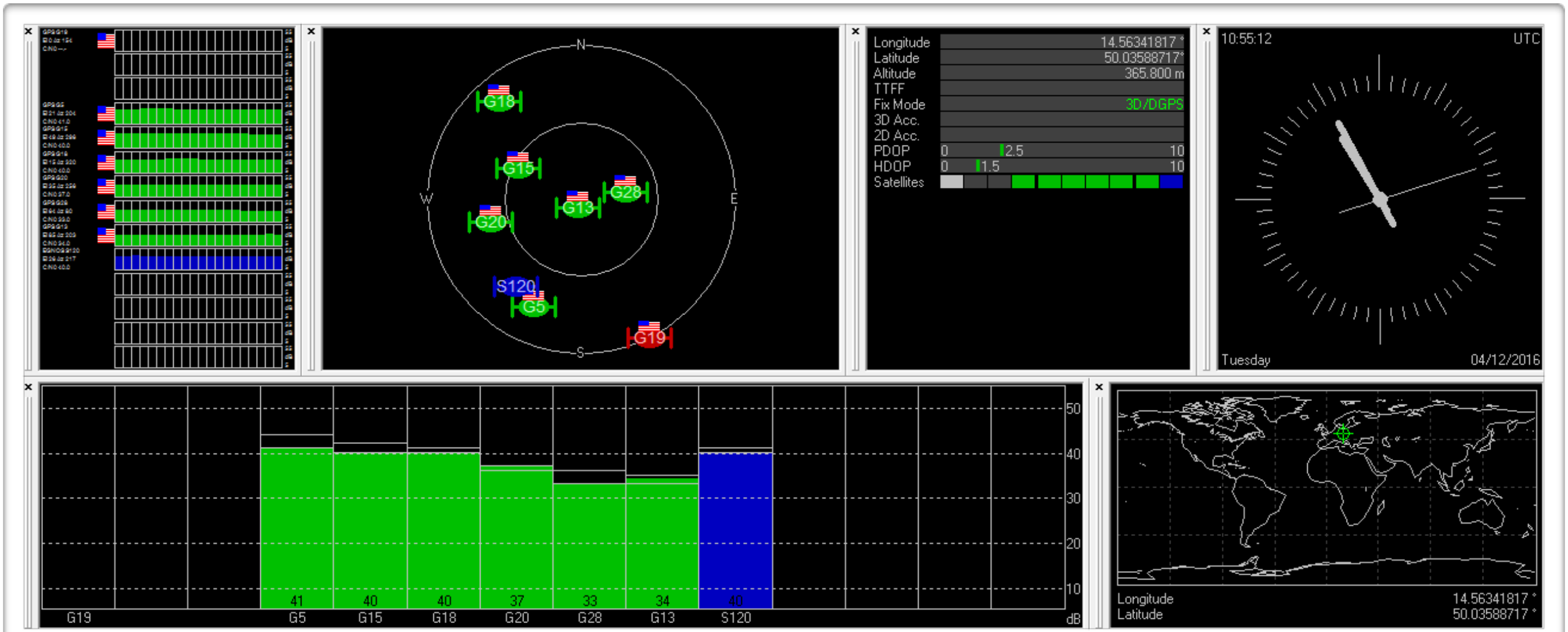


GNSS Replay Attack (Meaconing)





GPS L1 C/A Meaconing Verification



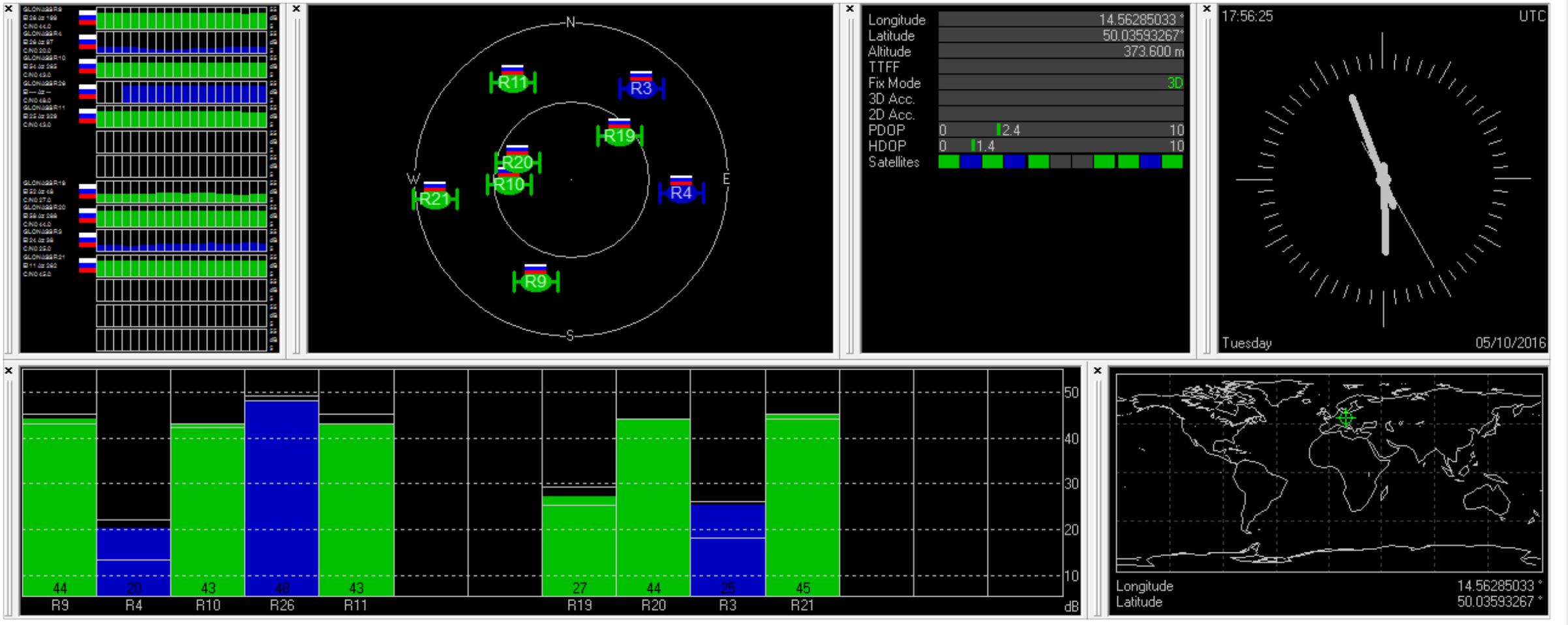
Note we have also successfully recorded the SBAS/EGNOS signal channel PRN120 coming from Inmarsat 3F2 AOR-E. The DGPS indicator above shows this signal has already been used for a fix assurance.

GLONASS L1OF Signal in Detail

Carrier frequency	L1: 1598.0625 - 1605.375 MHz, spacing by 562.5 kHz (14 carriers)
Minimum received power (GLONASS spc.)	-161.0 dBW = -131 dBm
Polarization	Right-Hand Circular Polarization (RHCP)
Multiple access	Frequency Division Multiple Access (FDMA)
Spreading modulation	BPSK-R(511 kHz)
Tx bandwidth	±511 kHz (first null-to-null BW)
Spreading codes	Common 511 bit m-sequence for all SVs
Data message structure	GLONASS
Data rate	50 bps
Data error control code	Extended (85,81) Hamming code
Data modulation	50 sps biphase modulation
Pilot and data components	100% power data
Overlay code	Meander sequence 101010… @ 100 bps
Multiplexing with other signals	In phase quadrature to L1SF

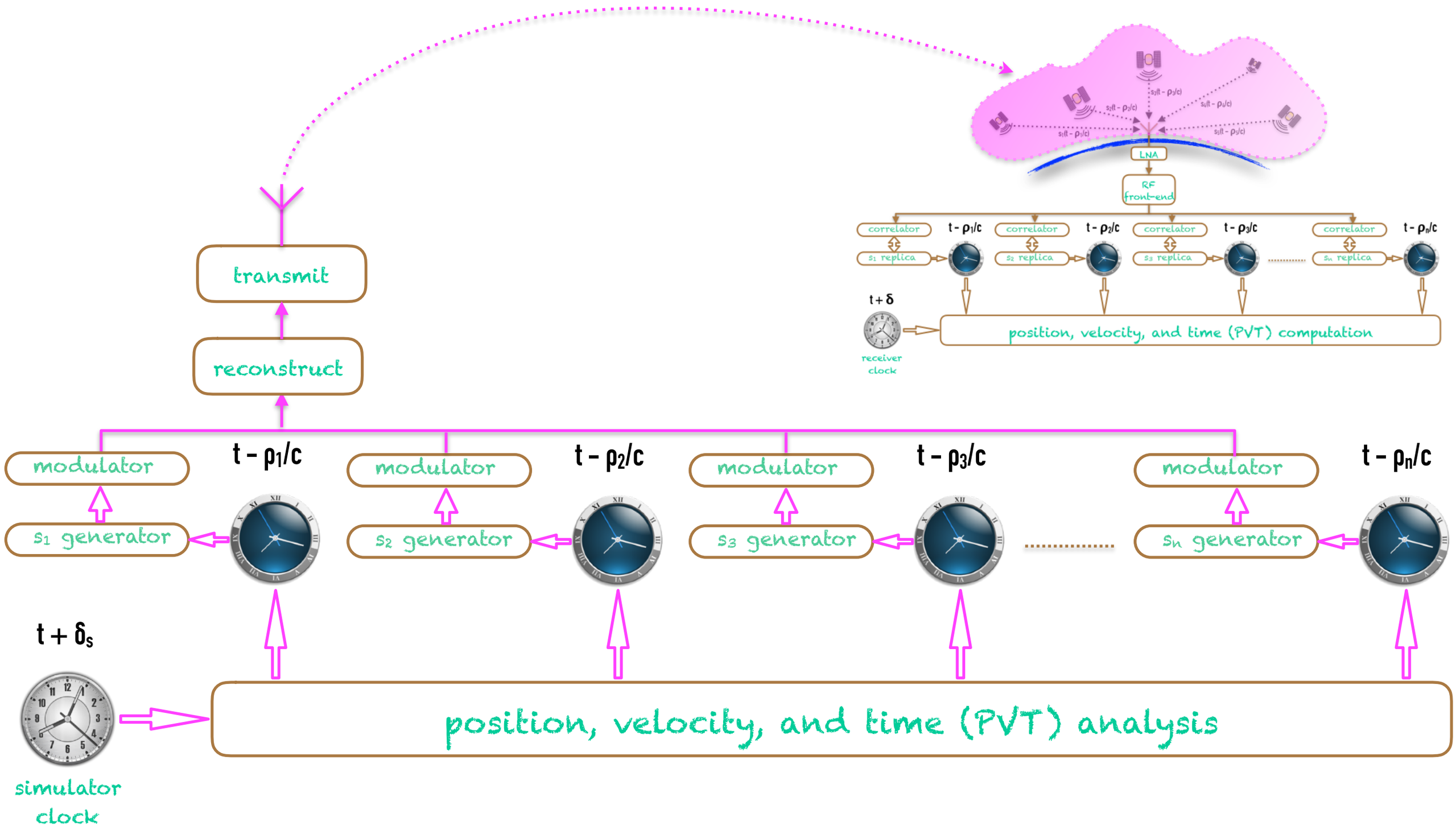
[Betz, 16], [GLONASS ICD, 08]

GLONASS L1OF Meaconing Result



Each SV in this view uses its own carrier frequency [GLONASS ICD, 08], however, we have recorded the whole FDMA multiplex centred at 1602 MHz with 8.333333... MHz bandwidth (adjusted for USRP N210 clock ratio) via bandpass signal complex sampling.

GNSS Spoofing Attack by Tracking Reversal



SBAS to the Rescue?

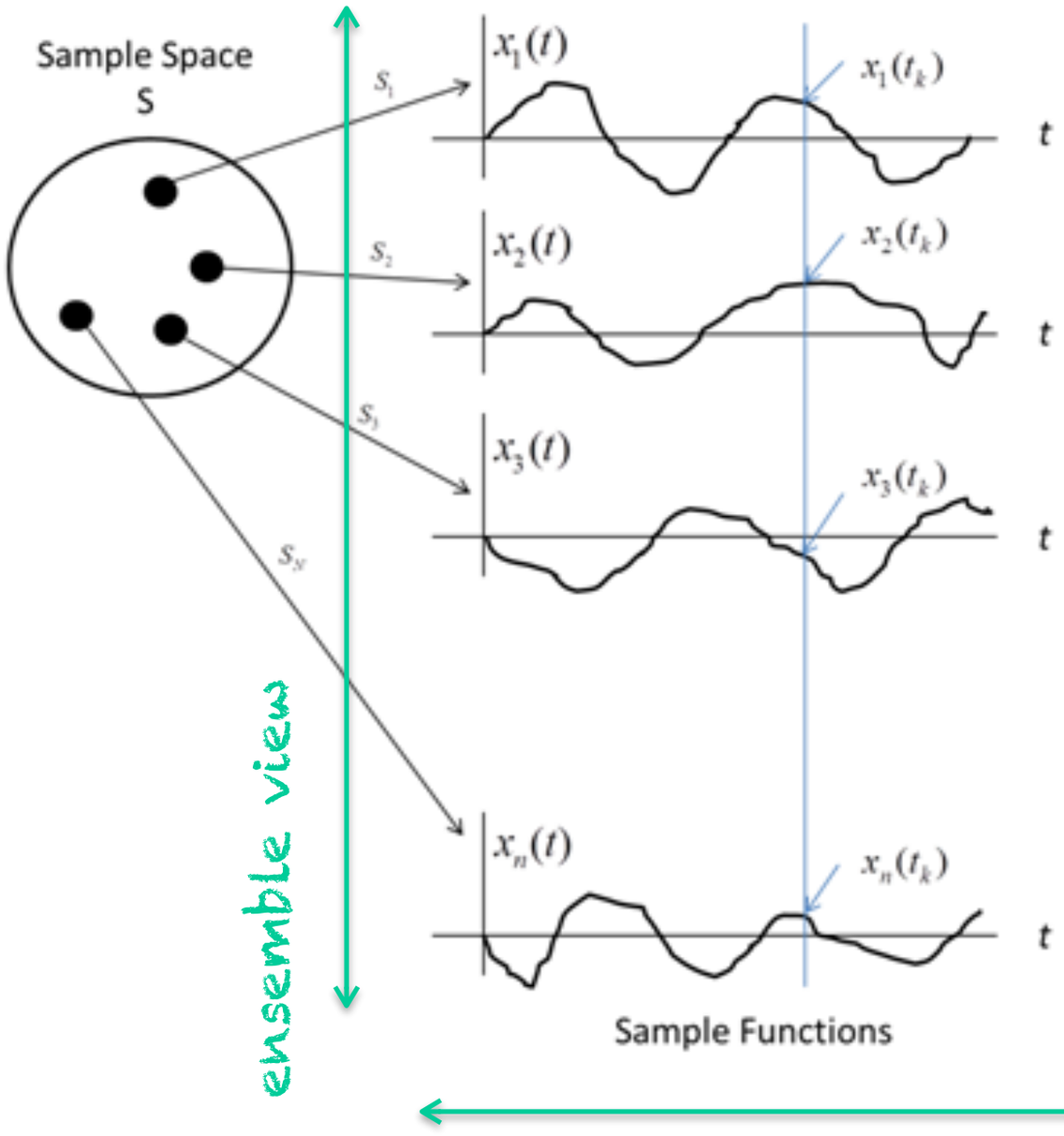
- Satellite-Based Augmentation System (in general)

  ... European Geostationary Navigation Overlay Service (EGNOS), for example, in particular

- Provides integrity report and differential corrections for the original L1 C/A signal

  ... however, it rather applies to the *transmitted signal*, instead of the signal received by the individual user station

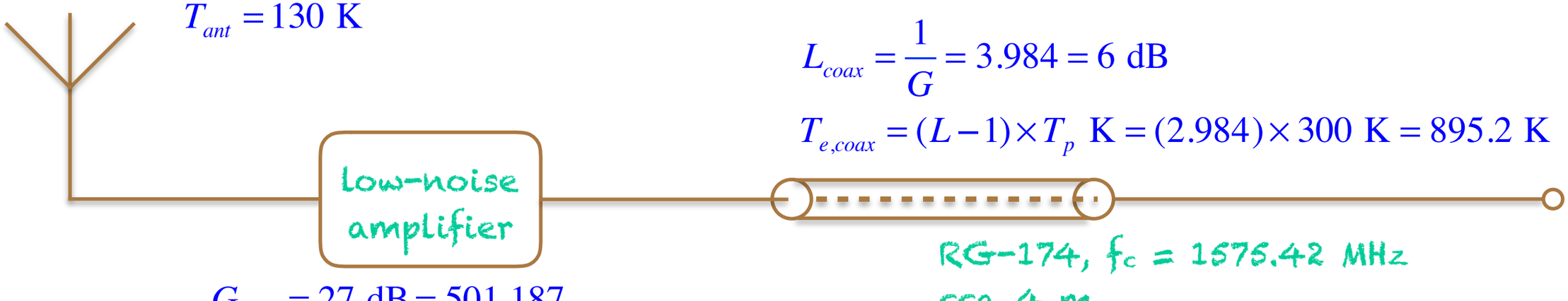
Noise in Electronic Circuits



- In general, we model such a signal as a realisation of a continuous- (or discrete-) time random process.
- That means, we observe successive measurements or projections of a randomly chosen internal state of the system (*time view*).
- For a given time instant t_k, $X(t_k)$ is a random variable (*ensemble view*).
- We call the process e.g. Gaussian, if $X(t_k)$ has such distribution.
- We shall be very careful with mixing time and ensemble views (cf. ergodic process properties).

[van Etten, 05]

Antenna-LNA-Coax Example



$T_{ant} = 130 \text{ K}$

$G_{LNA} = 27 \text{ dB} = 501.187$

$F_{LNA} = 1.8 \text{ dB} = 1.514$

$T_{e,LNA} = (F-1)\times 290 \text{ K} = (0.514)\times 290 \text{ K} = 149.06 \text{ K}$

$G_{coax} = -6 \text{ dB} = 0.251$

$L_{coax} = \frac{1}{G} = 3.984 = 6 \text{ dB}$

$T_{e,coax} = (L-1)\times T_p \text{ K} = (2.984)\times 300 \text{ K} = 895.2 \text{ K}$

$G = G_{LNA}G_{coax} = (27-6) \text{ dB} = 21 \text{ dB} = 125.893$

$T_e = T_{e,LNA} + \frac{T_{e,coax}}{G_{LNA}} = (149.06 + \frac{895.2}{501.187}) \text{ K} = 150{,}846 \text{ K}$

$T_i = T_{ant} + T_e = 280.846 \text{ K}$

$N_0 = kGT_i = 1.38\times 10^{-23}\times 125.893\times 280.846 \text{ WHz}^{-1} = 487.92\times 10^{-21} \text{ WHz}^{-1} = 487.92 \text{ zWHz}^{-1}$

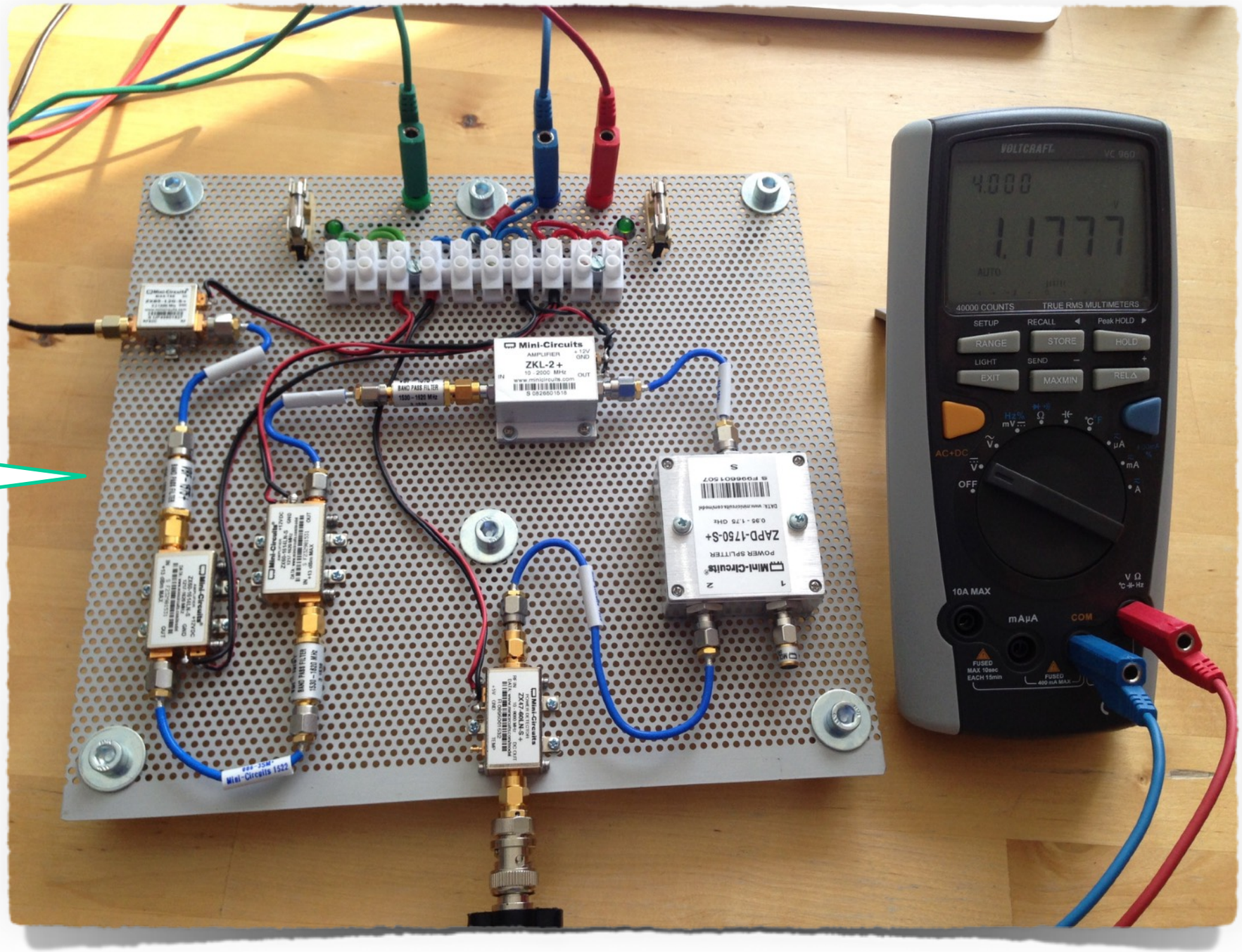
$= -153.117 \text{ dBm-Hz}$

RF Front-End Example

Besides the internal SDR RF board, we need such an external front-end due to the extremely weak GNSS signals.

Basically, this is a versatile LNA (1530 to 1620 MHz, 49 dB typ.) featuring bias-tee, power splitter, and RSSI monitor.

Its fully based on the Mini-Circuits(R) components, so anybody can easily build their own.



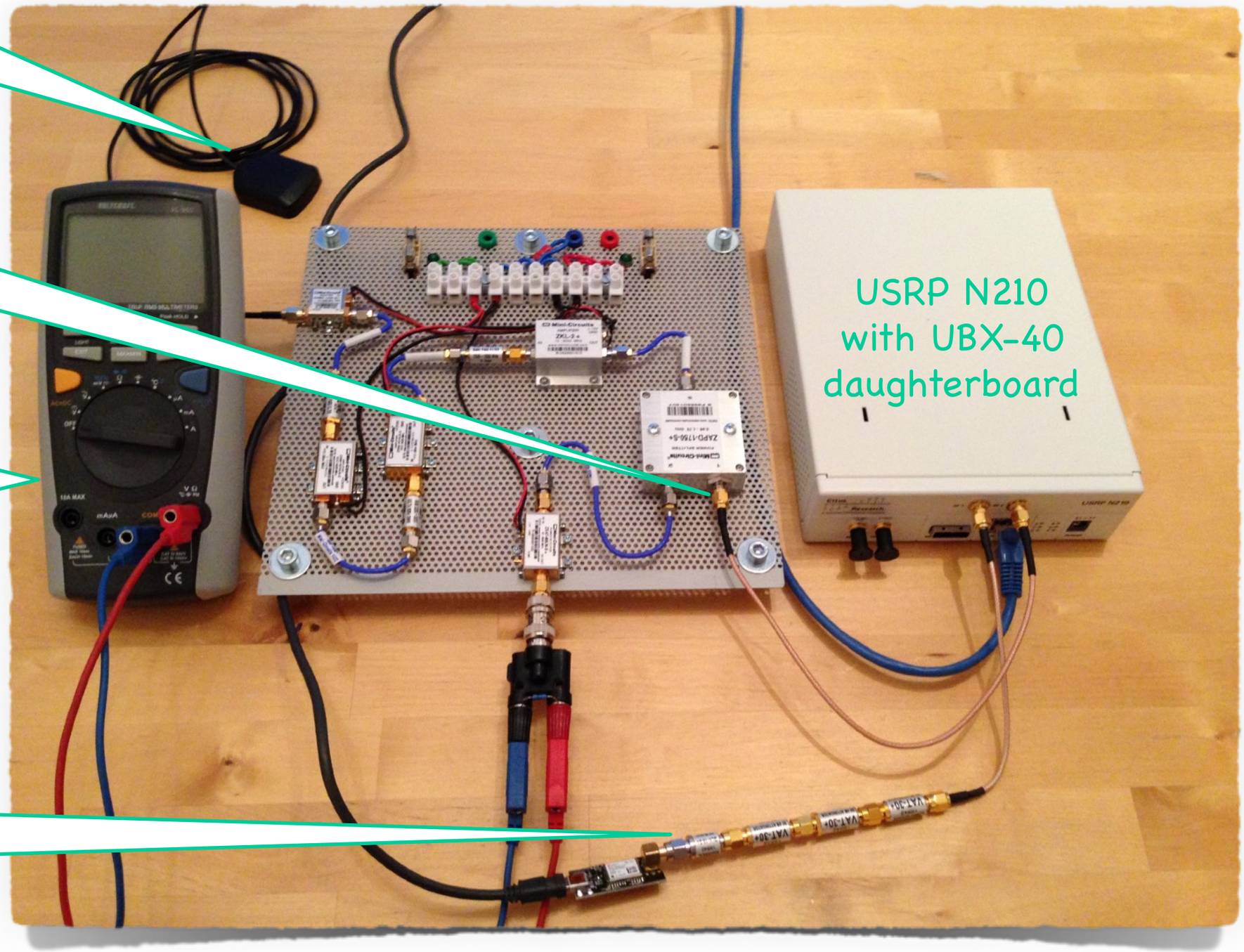
Record & Replay (Meaconing) Setup

Active antenna

Rx path delivers the original GNSS signal to be recored.

RSSI monitor checks the original RF signal received.

Later on, Tx path verifies the replayed signal with u-blox receiver. Don't forget the DC block and attenuators (3x30 dB in this case)!



So, Cryptography to the Rescue?

- It is a good initial guess, but despite having really rich cryptographic primitives portfolio nowadays, the remedy for GNSS is by no means straightforward.

- Easy-to-implement broadcast data origin authentication that is resistant to meaconing

... e.g. TESLA algorithm [Perring, et al., 02] and a suggestion for TESLA in Galileo Commercial Service (CS) enlightening the main issues [Hernandez, et al., 15]; cf. also studies in [Dovis, 15], [Humphreys, 13], [Wesson, 12]

And yes, please stop thinking like *encrypted* = *secured*!

Signal Space Cryptography

- **Instead of payload data, we need to protect the waveforms**

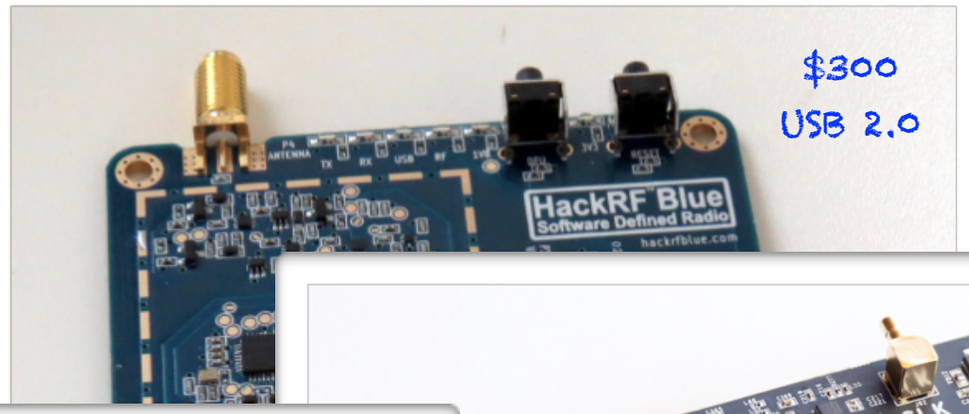
... cryptography seldom faces such a challenge; similar issues are connected with *distance bounding protocols*

- Deeper incorporation of cryptography into the modulation scheme is needed, provided - for instance - the prevention of even a partial signal tracking is our security goal

... as the semi-codeless tracking of L1/L2 P(Y) [Woo, 99] used routinely by e.g. EGNOS [Betz, 16] is actually nothing but a successful partial cryptanalysis of the military GPS signal protection scheme

Software Defined Radio

about $20 (NooElec)
RX only



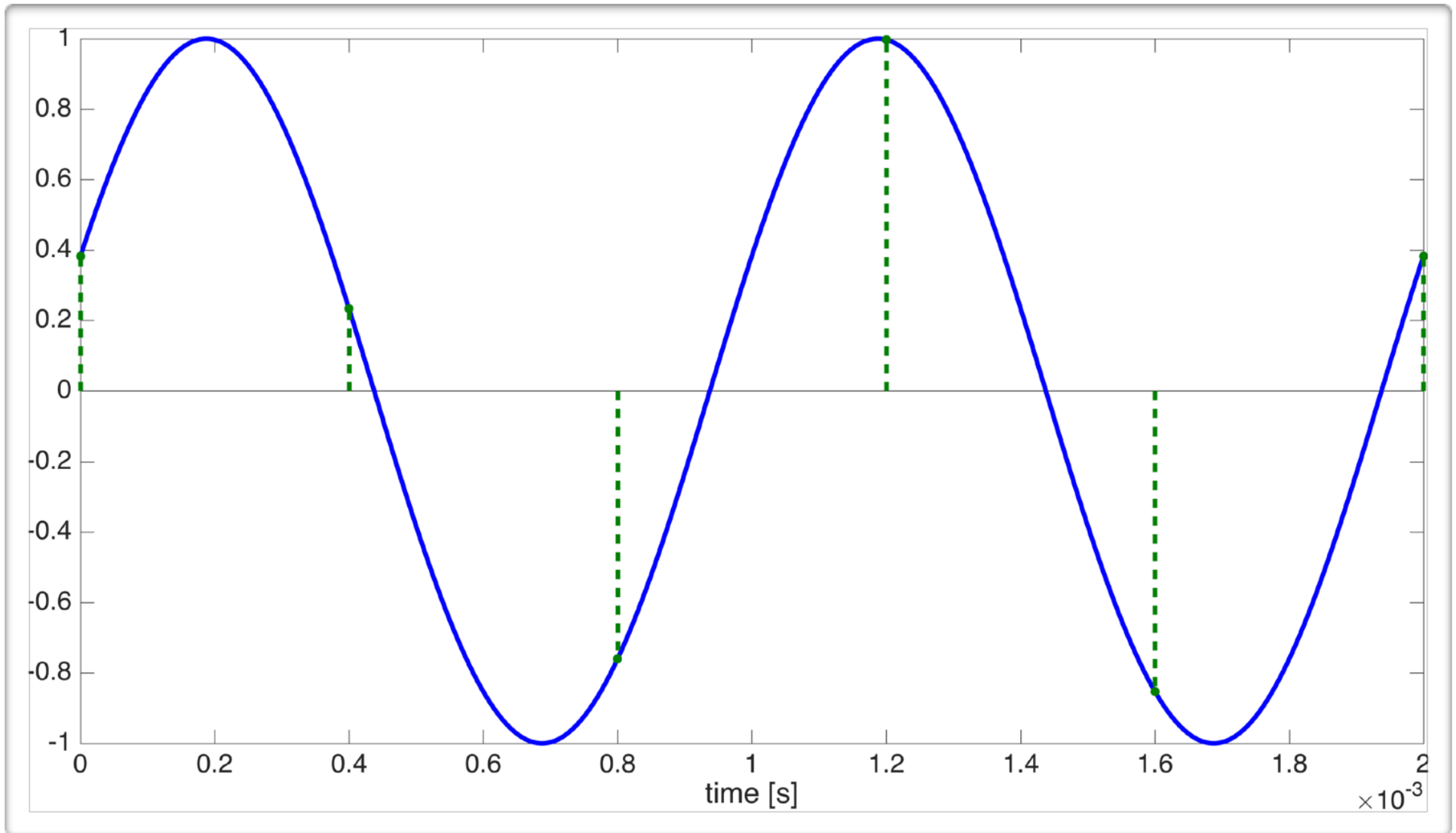
$300
USB 2.0

bladeRF $420 - 1500
USB 3.0

> $2000
1 GigE

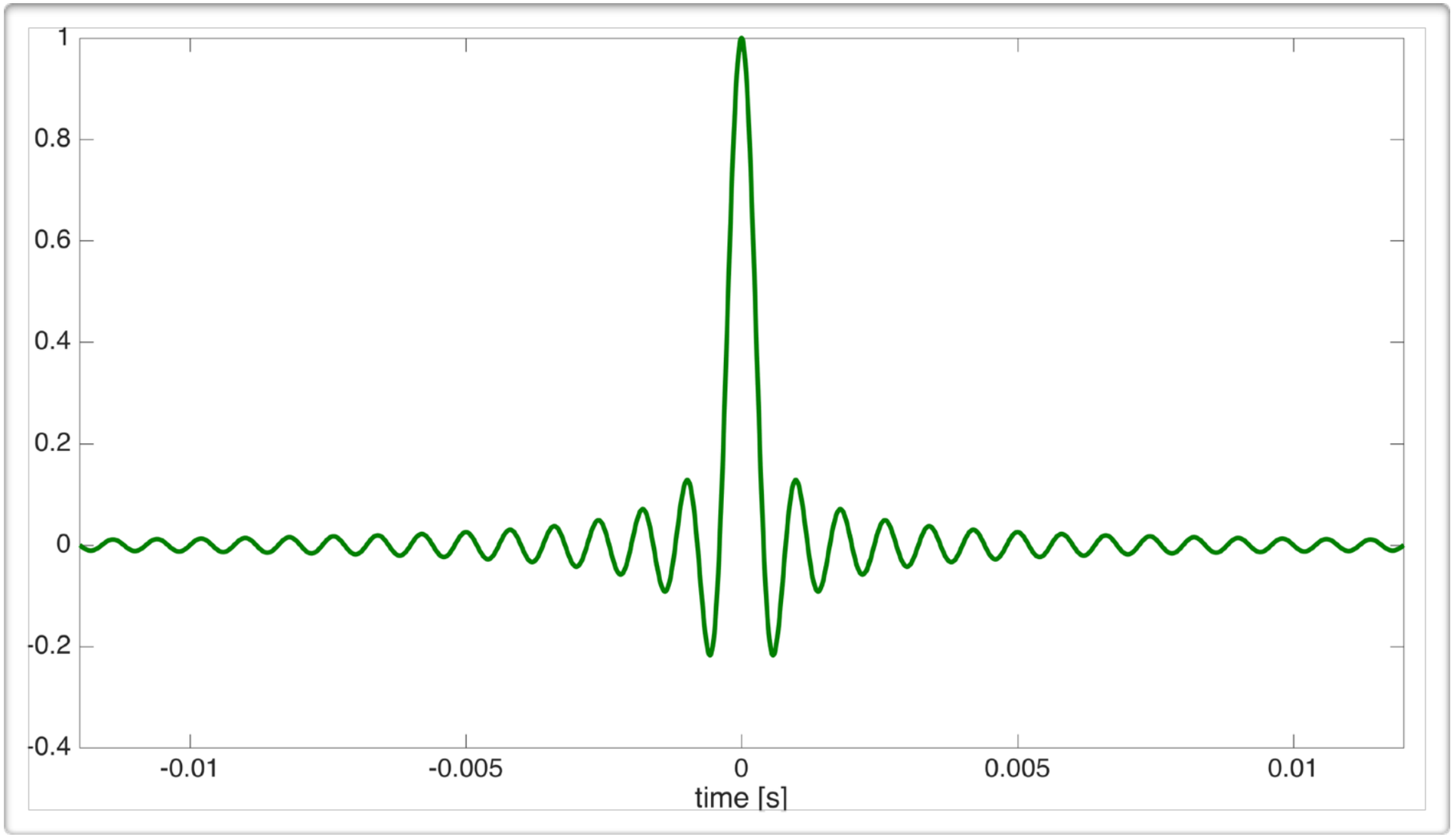
USRP B210 $1400
USB 3.0

Real Signal Sampling



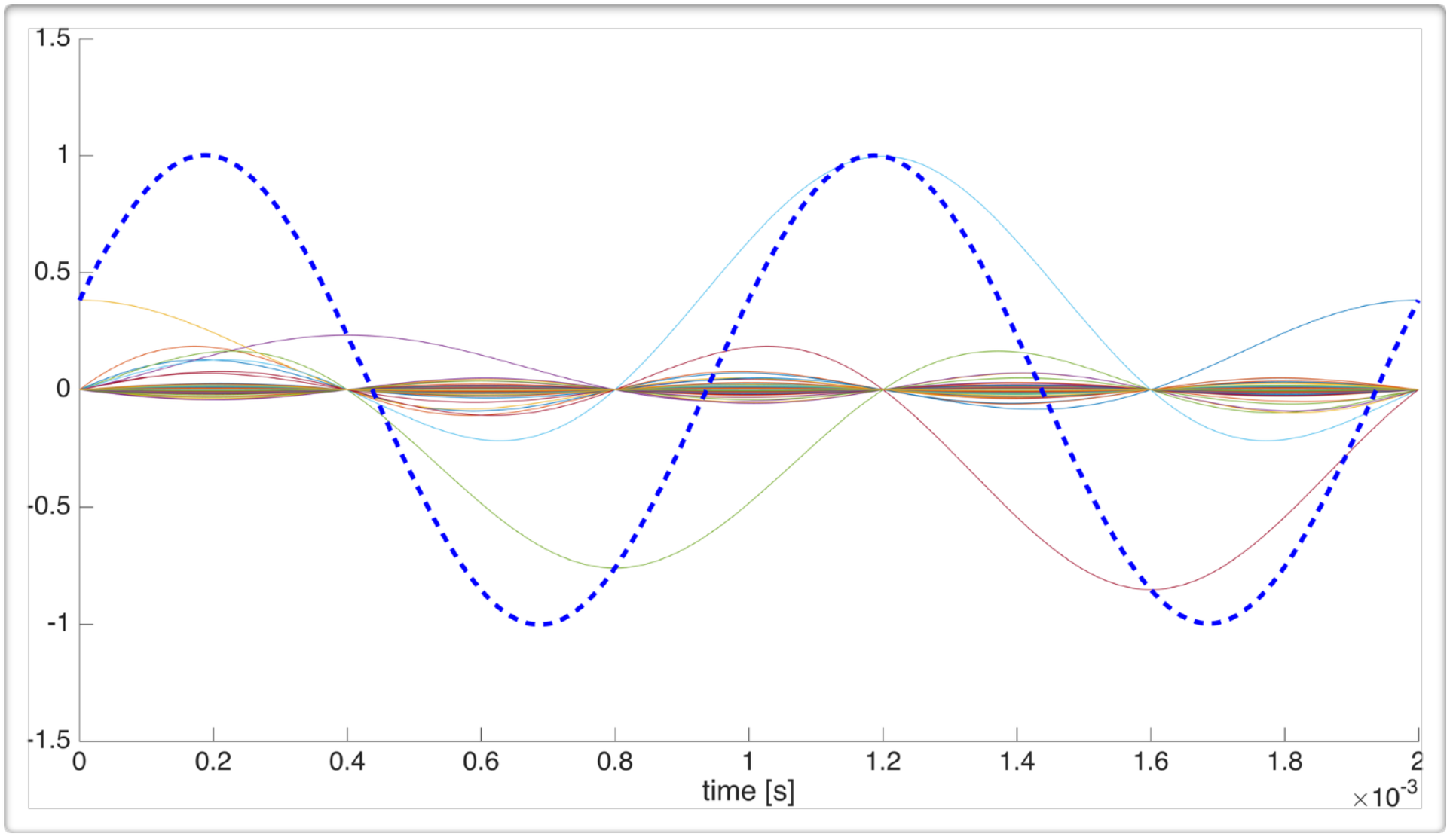
1 kHz harmonic signal sampled at f_s = 2.500 kHz

Sinus Cardinalis (sinc)



in lowpass filter impulse response time-scale for f_s = 2.500 kHz

Real Signal Reconstruction



interpolation by shifted and scaled replicas of sinc at f_s = 2.500 kHz time-scale with finite 30-sample delay

Complex or Real?

- In general, $s(t)$ can be a complex-valued function of a real time value. We then have:

$$s(t) = x(t) + iy(t)$$

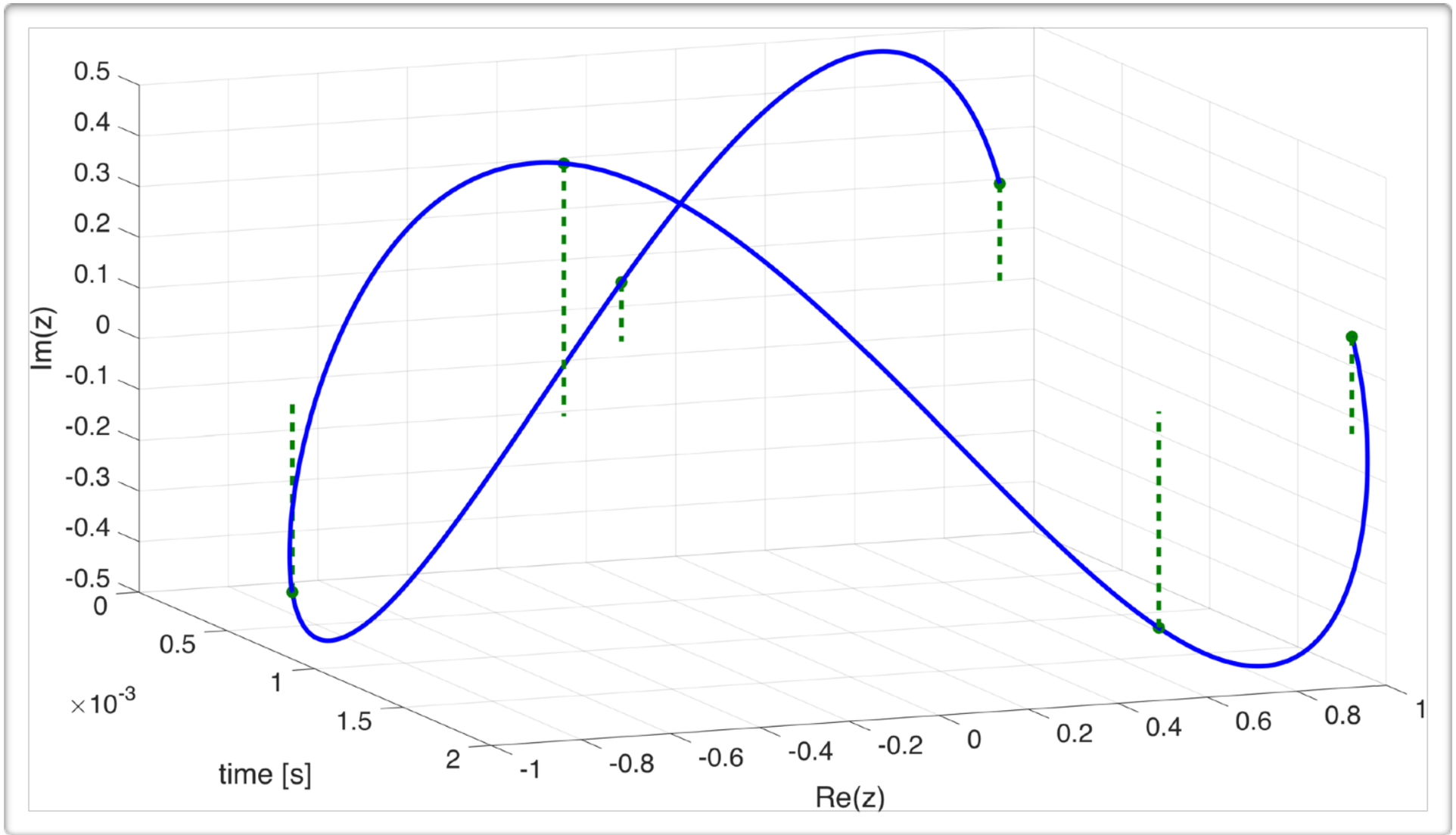
where $x(t)$ and $y(t)$ are real functions of the continuous time.

... also called in-phase (I) and quadrature (Q) components, respectively

... we need I/Q signal processing to describe the baseband envelope of a bandpass signal, since such a signal cannot be generally expected to have the Hermitian spectrum symmetry

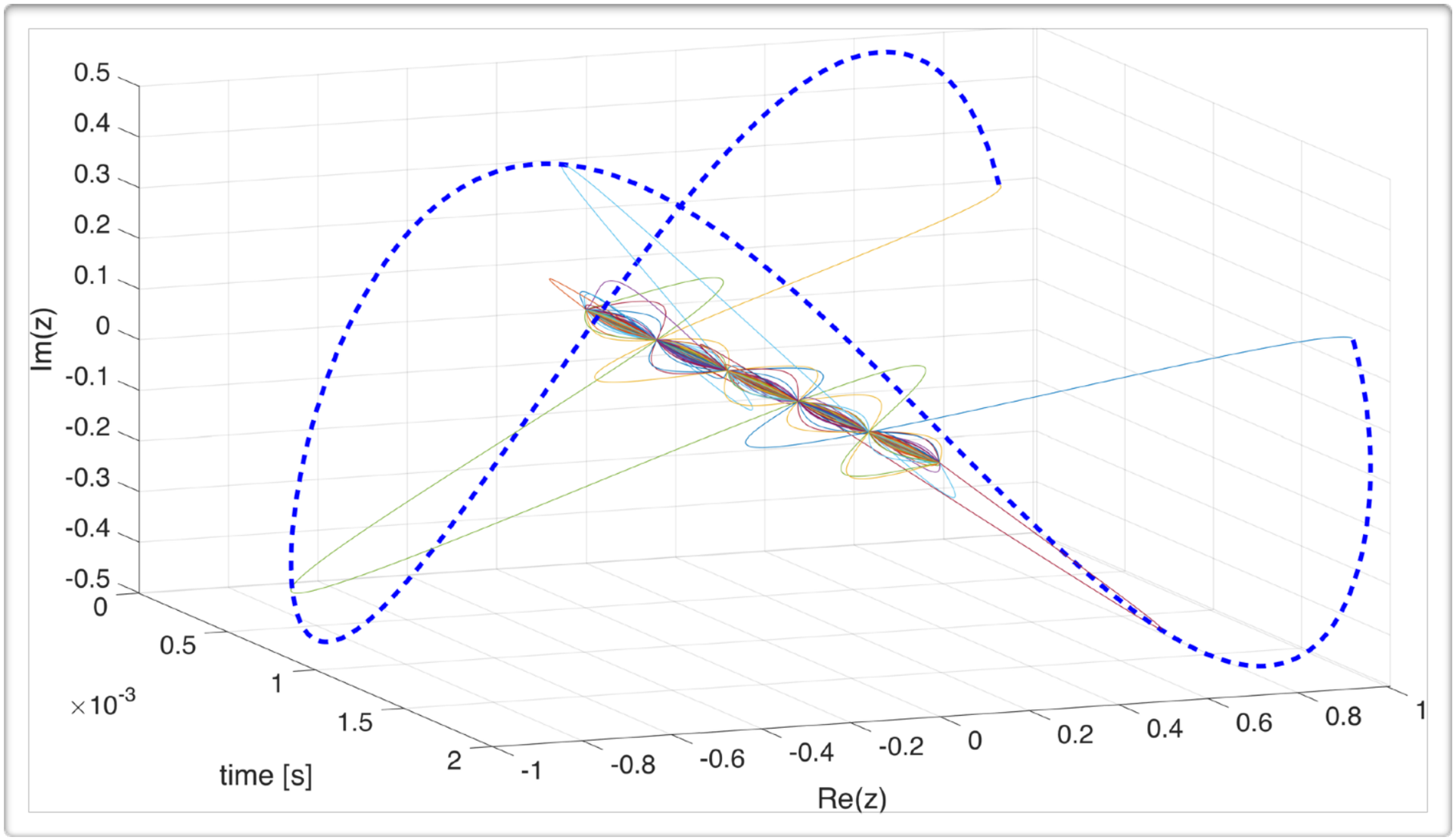
... by substituting this $s(t)$ into the sampling theorem equation, we see we can actually work with I/Q parts separately as with two components of the complex vector $s(t)$ on $\boldsymbol{C}_{\mathrm{R}}$ space with its standard basis $\{\mathbf{1}, \boldsymbol{i}\}$

Complex Signal Sampling



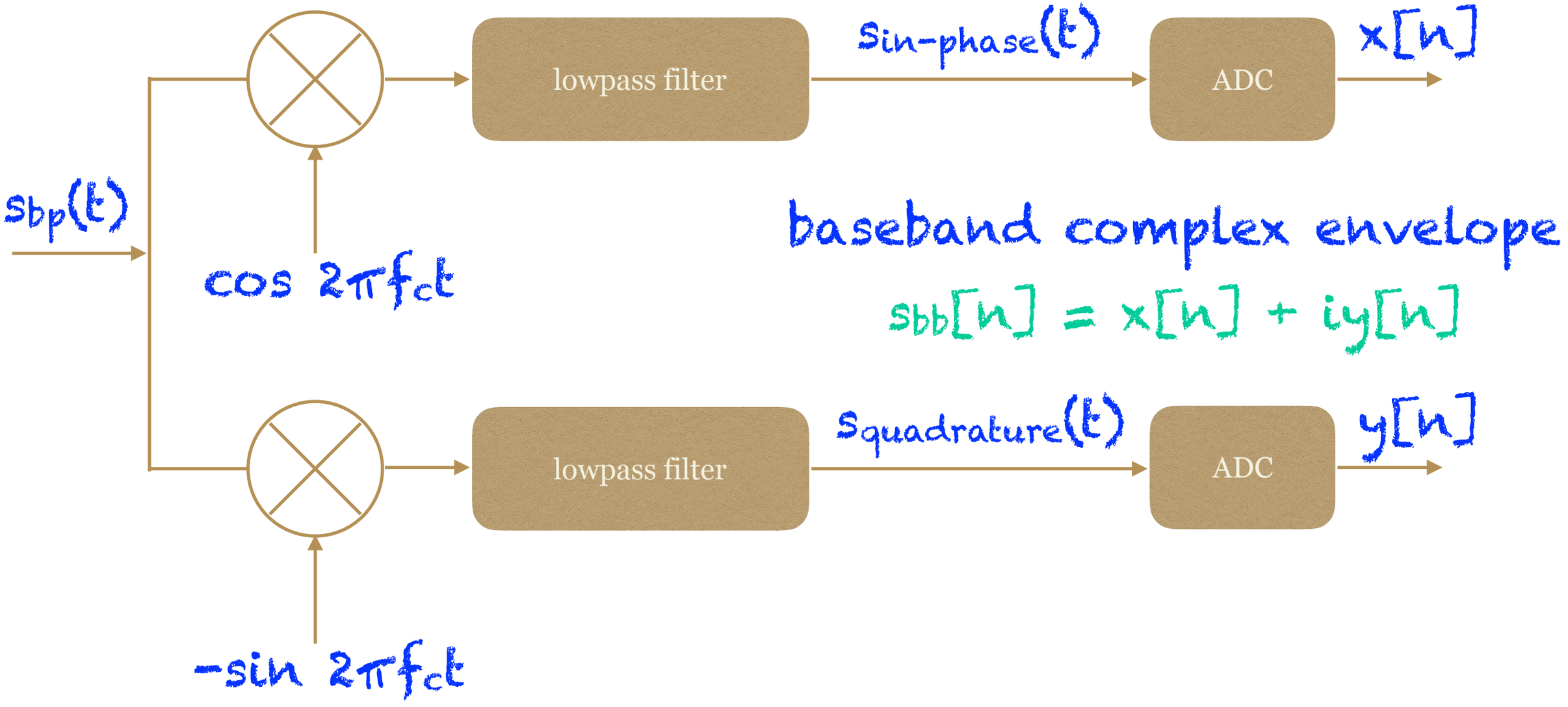
complex signal sampled at f_s = 2.500 kHz

Complex Signal Reconstruction



real and imaginary vector components interpolation
at f_s = 2.500 kHz with finite 30-sample delay

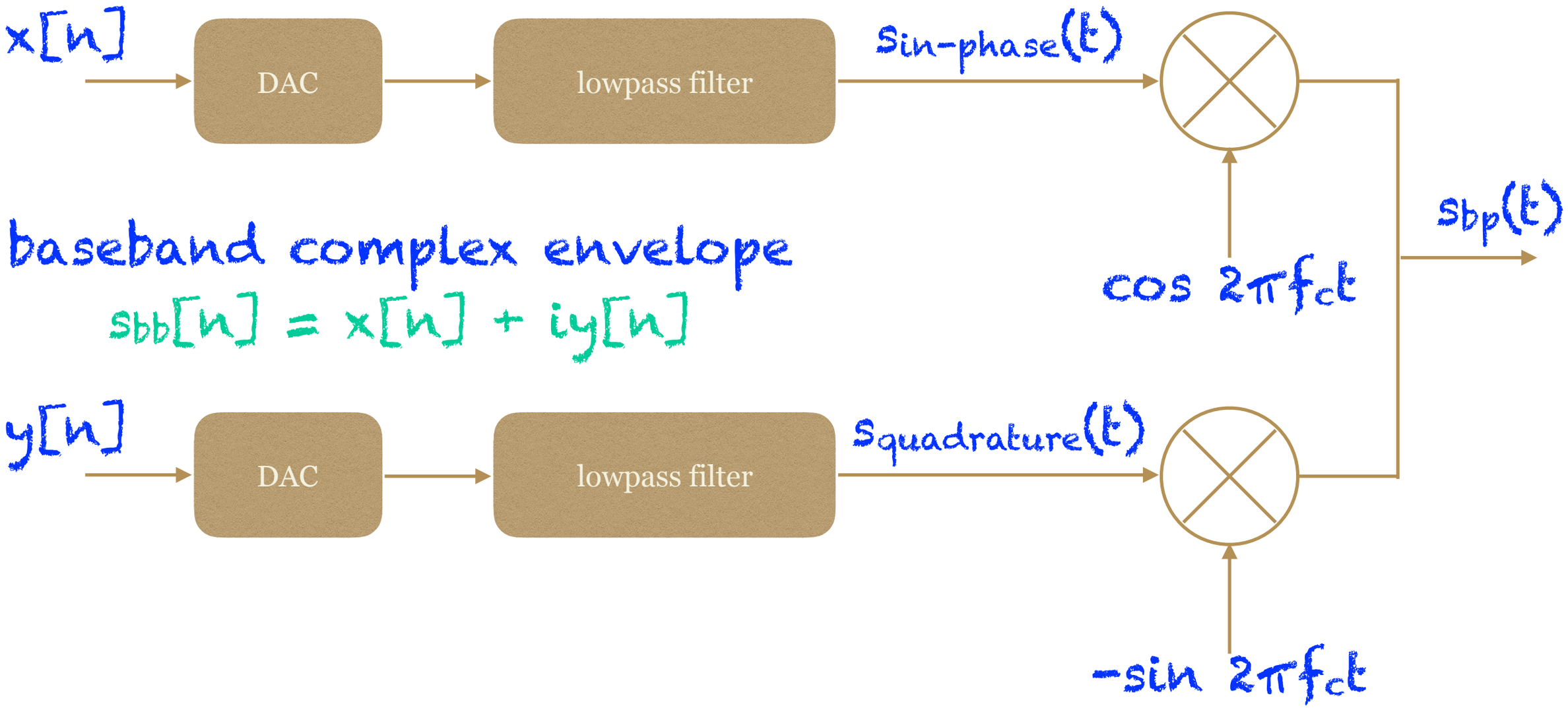
Bandpass Signal Quadrature (Complex) Sampling



bandpass signal complex downconversion ($f_c \rightarrow 0$ Hz)
and sampling at $f_s > B$

cf. [Lyons, 2011] for an excellent, accessible explanation

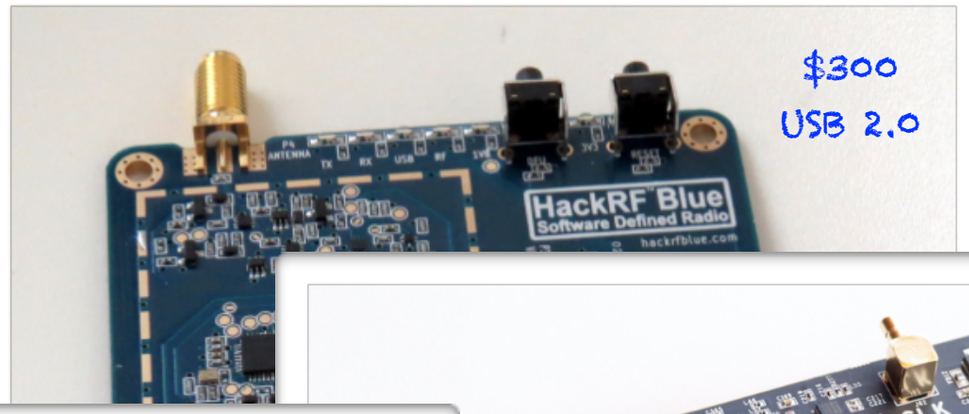
Bandpass Signal Reconstruction (Quadrature Modulation)



cf. [Lyons, 11] for an excellent, accessible explanation, [Johnson, Jr. et al., 11] for SDR context, [Holmes, 07] for GNSS applications

Software Defined Radio

about $20 (NooElec)
RX only



$300
USB 2.0

bladeRF $420 - 1500
USB 3.0

> $2000
1 GigE

USRP B210 $1400
USB 3.0

SDR as a Threat

DSP routines are SW. This can be shared, installed, and executed all around the world instantly with a very modest background.

Just like any other exploit code.

Conclusion

- **Software-defined radio breaks the barrier in between eager hackers and security-by-obscurity radio systems**

  ... what used to be a question of deep radio understanding and practical HW skills, is now a question of a few off-the-shelf components, basic course in DSP, and widespread SW frameworks for SDR

  ... in this light, the risk of many RF applications is clearly underestimated

- **Together with GSM, the GPS - as well as other GNSS - civil services seem to be among the first victims of emerging massive attacks**

  ... hopefully, Galileo Open Service (OS) will offer accessible and robust countermeasures even(!) for non-governmental applications

  ... as it would be clearly pointless to invest such a huge effort into a brand new service that would be de facto broken by design, now*

*) The Galileo Open Service protection (OS-NMA) is still "under construction", with little or no convincing cryptanalysis -> opportunity for you...