DINPAS GNSS Threats and Countermeasures

December 08, 2021
Philipp Richter

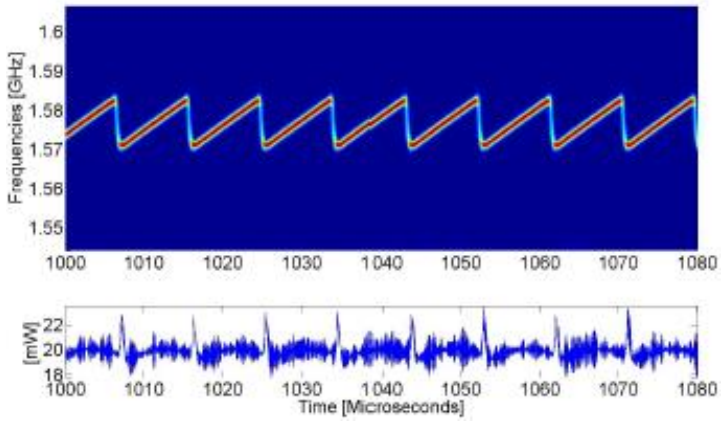
Outline

GNSS in todays infrastructure

- Several sectors rely on accurate position, velocity and time
  - Mobility
  - Logistics
  - Wireless communications
  - Data centers
  - Financial sector

Jamming

- Any signal with ‘enough’ power
- Common jamming signal types:
  - CW tones
  - pulsed signals
  - chirp
  - broadband



[1] Signal Characteristics of Civil GPS Jammers , Proceedings of ION GNSS, Portland, Oregon, 2011
[2] https://www.jammer-buy.com/gps-jammer/p-6967.html

Spoofing

README.md

GPS-SDR-SIM

GPS-SDR-SIM generates GPS baseb[redacted]ch can be converted to RF using software-defined radio (SDR) platforms, such as ADALM-Pluto, bladeRF, HackRF, and USRP.

Windows build instructions

1. Start Visual Studio.
2. Create an empty project for a console application.
3. On the Solution Explorer at right, add "gpssim.c" and "getopt.c" to the Souce Files folder.
4. Select "Release" in Solution Configurations drop-down list.
5. Build the solution.

Building with GCC

```
$ gcc gpssim.c -lm -O3 -o gps-sdr-sim
```

Using bigger user motion files

In order to use user motion files with more than 30000 samples (at 10Hz), the `USER_MOTION_SIZE` variable can be set to the maximum time of the user motion file in seconds. It is advisable to do this using make so gps-sdr-bin can update the size when needed. e.g:

```
$ make USER_MOTION_SIZE=4000
```

This variable can also be set when compiling directly with GCC:

```
$ gcc gpssim.c -lm -O3 -o gps-sdr-sim -DUSER_MOTION_SIZE=4000
```

Generating the GPS signal file

A user-defined trajectory can be specified in either a CSV file, which contains the Earth-centered Earth-fixed (ECEF) user positions, or an NMEA GGA stream. The sampling rate of the user motion has to be 10Hz. The user is also abl to assign a static location directly through the command line.

HackRF One

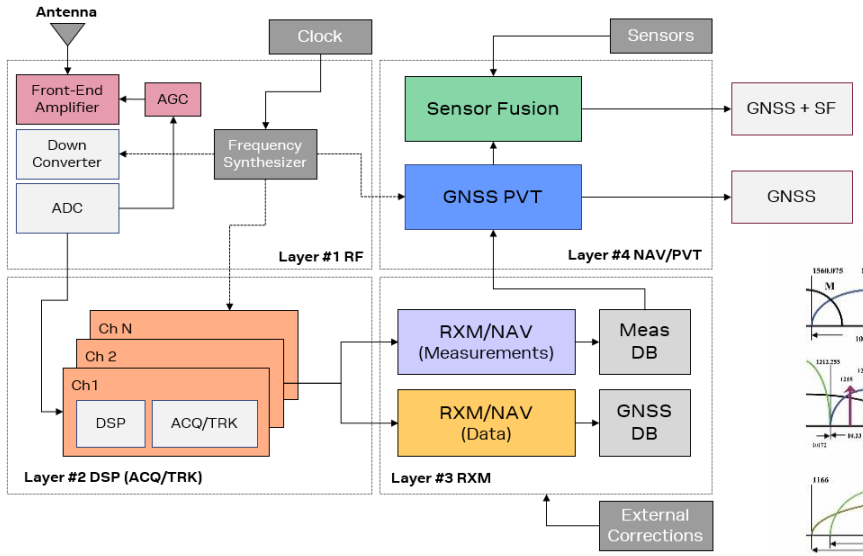
HackRF One from Great Scott Gadgets is a Software Defined Radio peripheral capable of transmission or reception of radio signals fr MHz to 6 GHz. Designed to enable test and development of modern and next generation radio technologies, HackRF One is an open hardware platform that can be used as a USB peripheral or programmed for stand-alone operation.

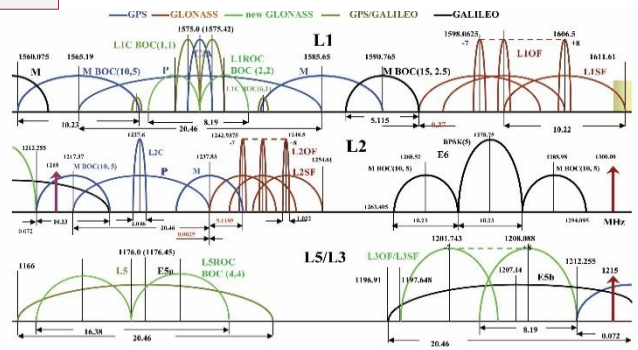
- 1 MHz to 6 GHz operating frequency
- half-duplex transceiver
- up to 20 million samples per second
- 8-bit quadrature samples (8-bit I and 8-bit Q)
- compatible with GNU Radio, SDR#, and more
- software-configurable RX and TX gain and baseband filter
- software-controlled antenna port power (50 mA at 3.3 V)
- SMA female antenna connector

Spoofing signals

Onset of attack, capture tracking loops:

- signal denial
- overpower
- lift-off (carry-off)





Consistency with live-sky:

- alignment in Power and Time
- Navigation data
- between signals, signals of constellations, signals in different bands

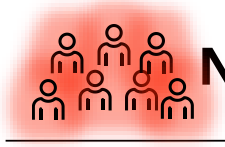
Consistency with models and receiver motion, e.g.:

- noise floor, rate of code phase
- clock characteristics
- position/velocity, **…**

❖ Consistency vs Complexity

❖ Receiver vs Spoofer capabilities

Threat actors

Type	Motivation	Capability
 **Privacy Seekers** **Script Kiddies**	• Privacy • Boredom	• Low
 **Hacktivists**	• Political	• Medium
 **Researchers**	• Improve security • Self-marketing	• High
 **Cybercriminals**	• Financial	• High
 **Nation state**	• Damage foreign systems	• Advanced

Impact

- Jamming
  - Unintentional interference
  - Intentional jamming
- Spoofing
  - Meaconing (rebroadcasting)
  - Broadcasting fake signals
- GNSS system issues
  - December 2020: Galileo ground system atomic clock failure
  - January 2016: GPS UTC parameter error

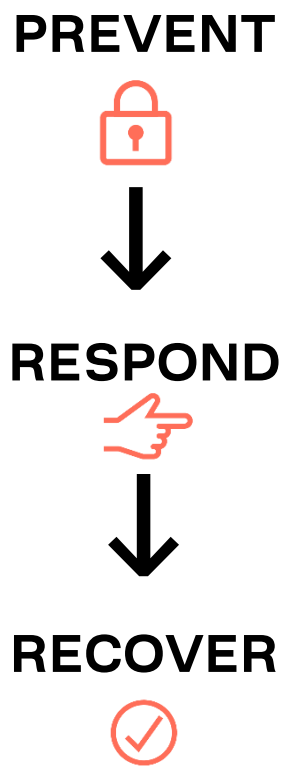
- ➢ Impact can vary from increased noise to denial of service
- ➢ CW jamming – ghost satellites

- ➢ Impact can vary from nothing to false PVT to no PVT

- ➢ Large PVT errors
- ➢ Service not available
- ➢ …

Jamming countermeasures

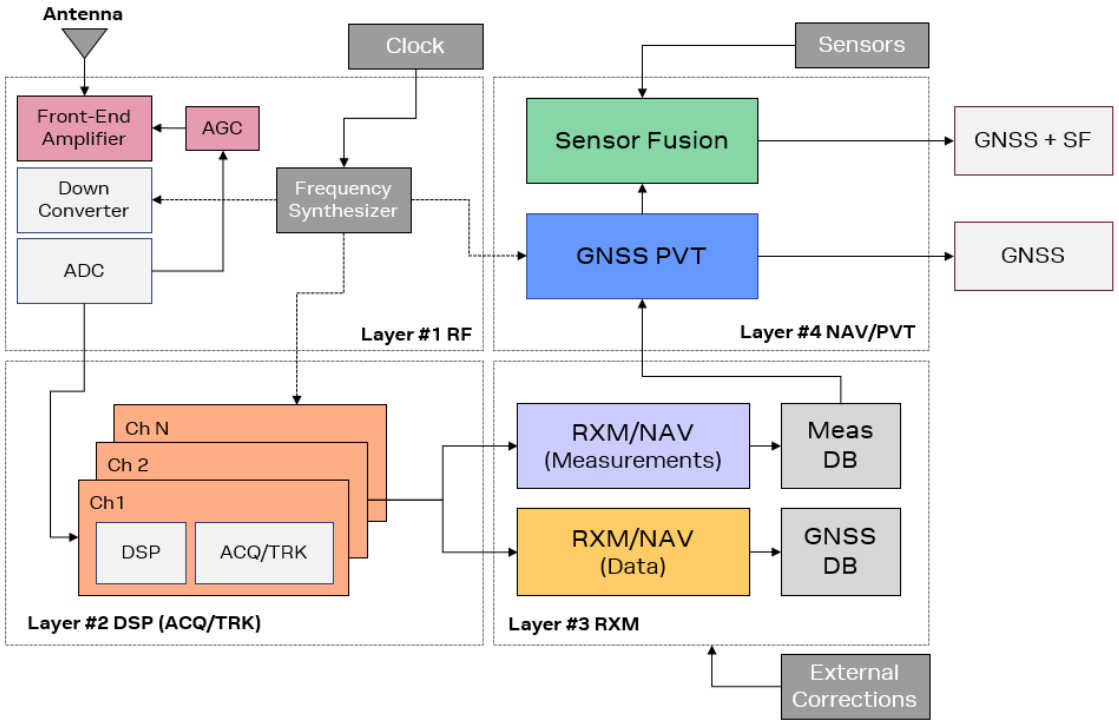
- Adaptive antenna systems, null steering antennas
- Out-of-band interference:
  - RF front-end filtering
- In-band jamming:
  - Adaptive filtering
    - Static/slow varying CW and narrowband jammers
    - Adaptive notch filters against fast chirp jammers
  - Multi-band receiver may switch to un-jammed band
- Monitor AGC, power levels, signal spectrum
- Recover after attack



Spoofing countermeasures

GNSS receiver processing chain

- Antenna
- RF
- Signal processing
- Broadcast data message
- Navigation processing
- Host system

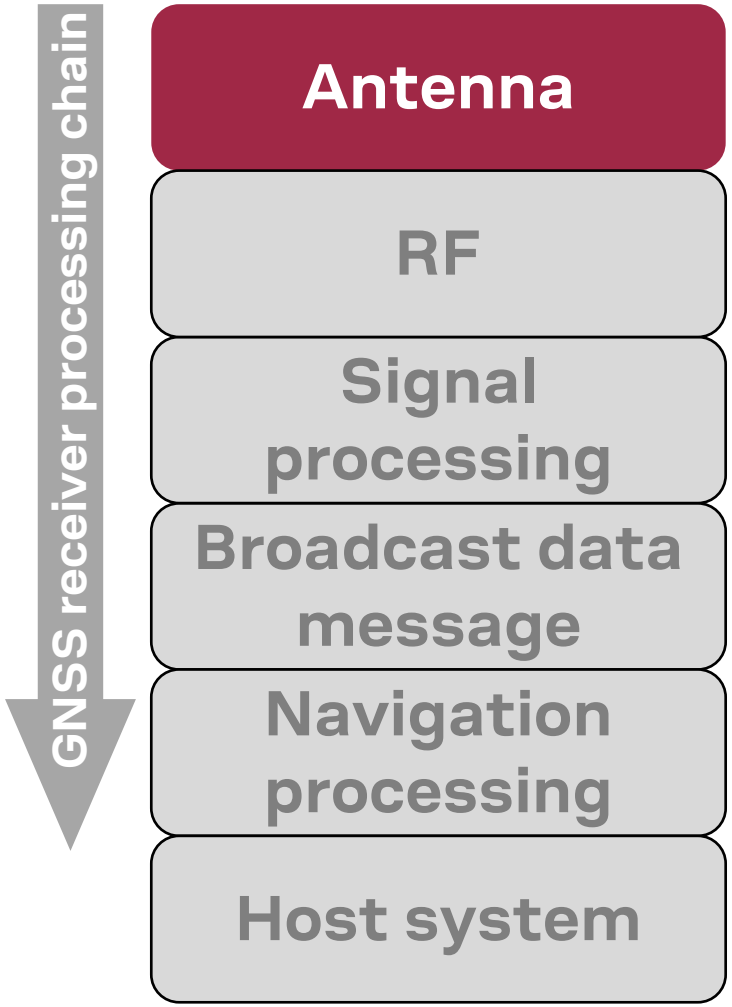


PREVENT

RESPOND

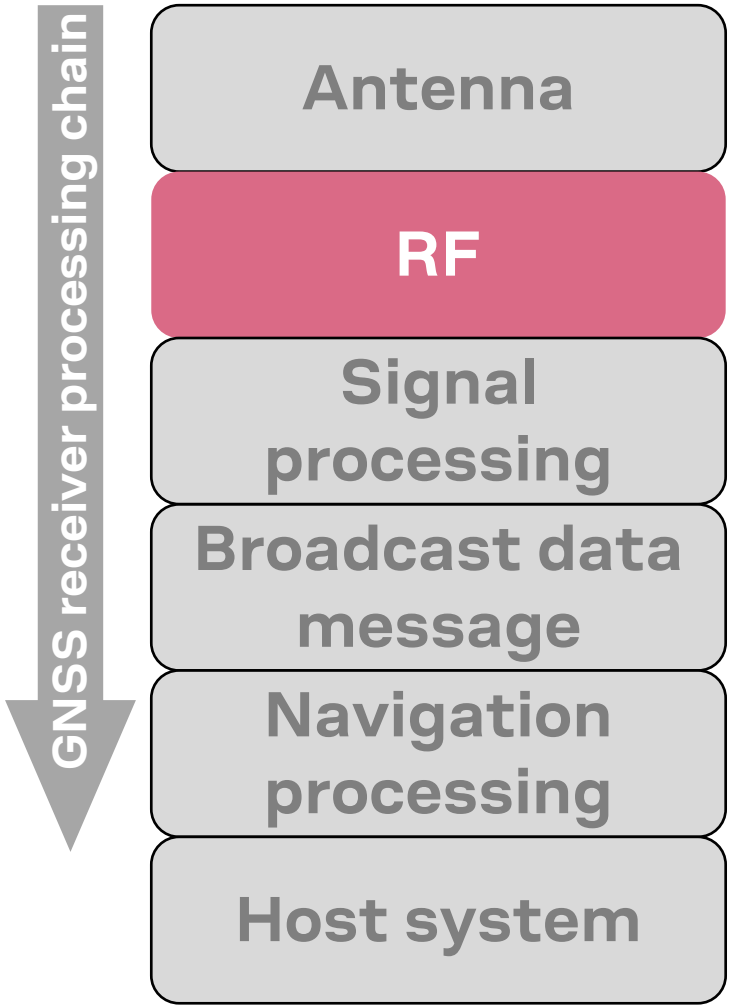
RECOVER

Spoofing countermeasures



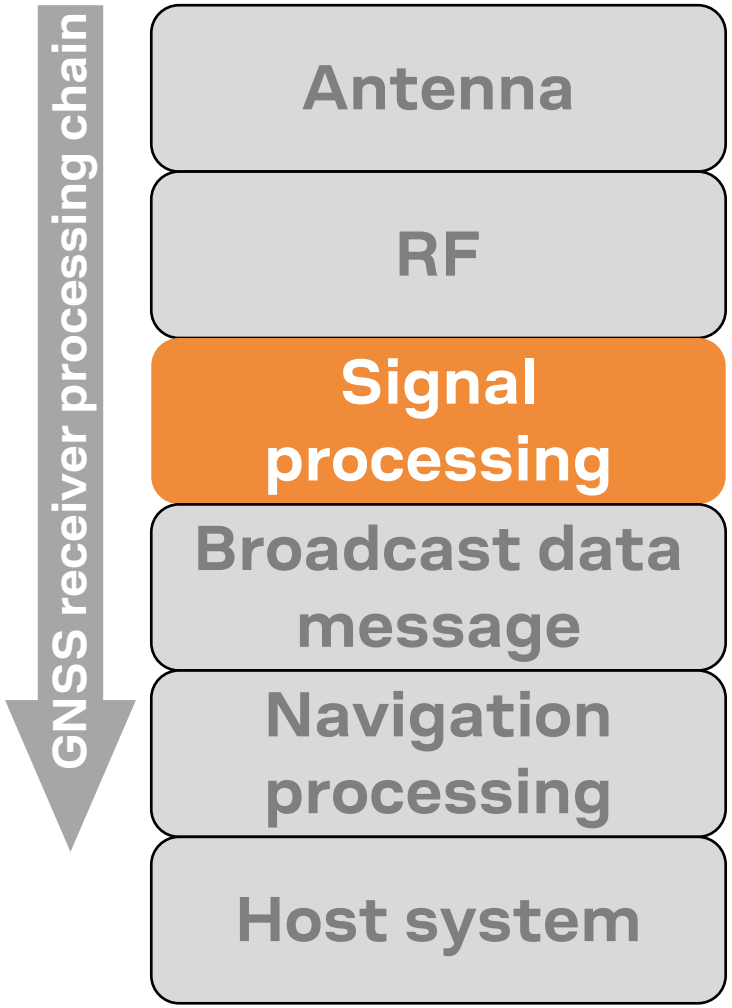
- Antenna arrays for angle-of-arrival detection

Spoofing countermeasures



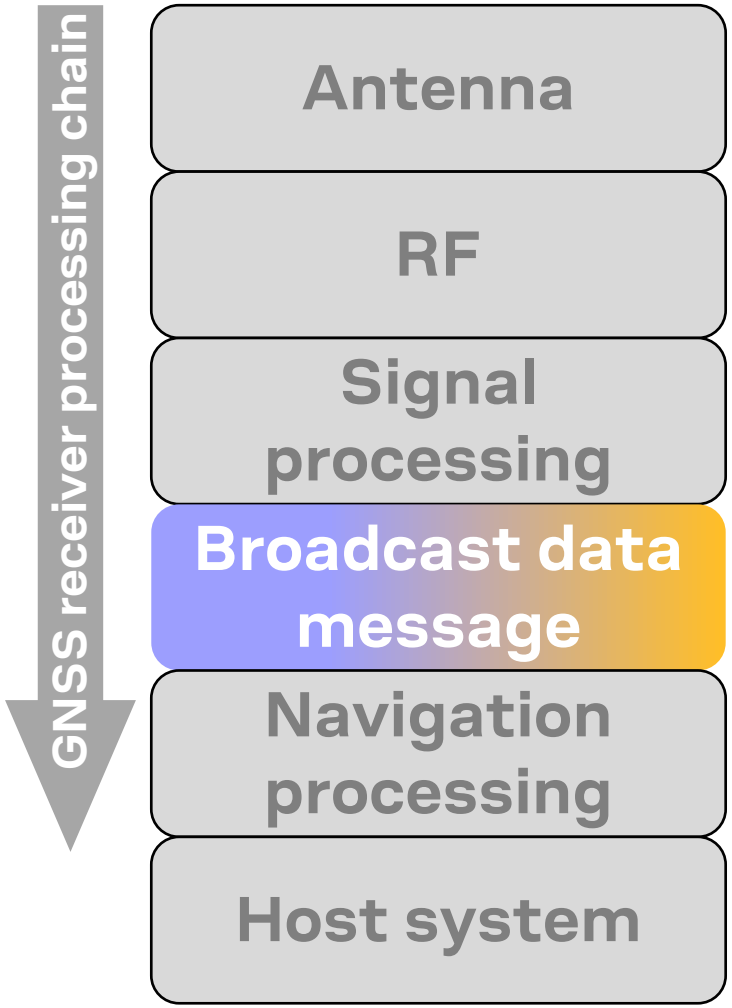
- Antenna arrays for angle-of-arrival detection
- Power level and spectrum checks
  - Changes over time, between GNSS and frequency bands

Spoofing countermeasures



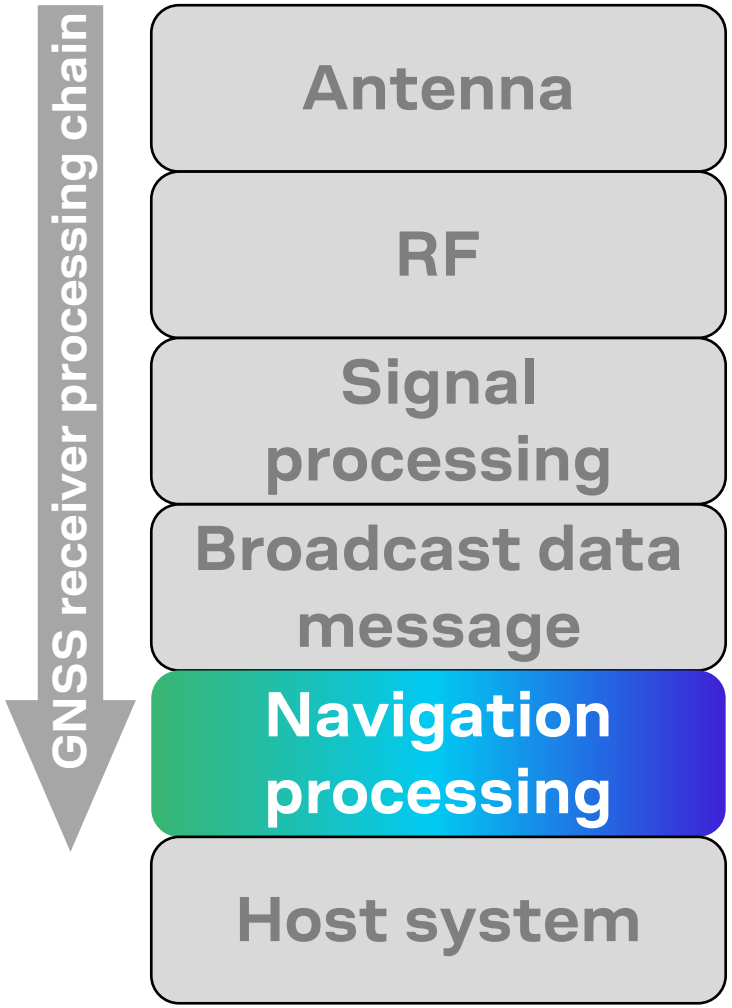
- Antenna arrays for angle-of-arrival detection
- Power level and spectrum checks
  - Changes over time, between GNSS and frequency bands
- Signal quality and consistency monitoring
  - Between GNSS systems and frequency bands

Spoofing countermeasures



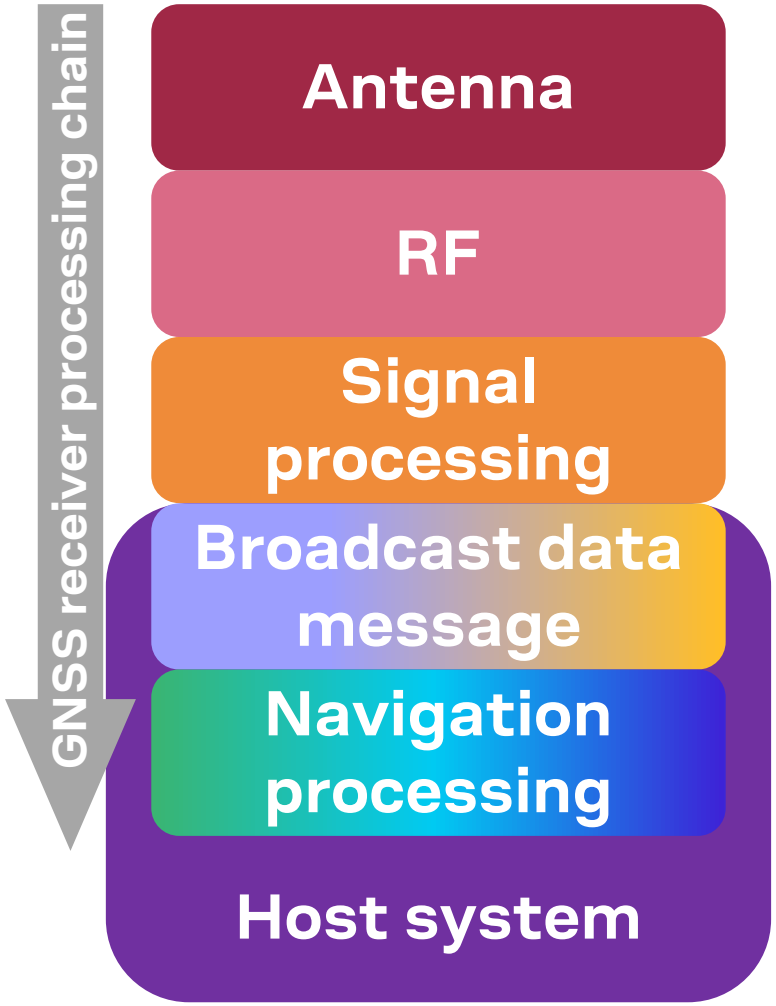
- Antenna arrays for angle-of-arrival detection
- Power level and spectrum checks
  - Changes over time, between GNSS and frequency bands
- Signal quality and consistency monitoring
  - Between GNSS systems and frequency bands
- Navigation data validity checks (eg DHS whitelist)
- Navigation data authentication (Galileo OS-NMA)

Spoofing countermeasures



- Antenna arrays for angle-of-arrival detection
- Power level and spectrum checks
  - Changes over time, between GNSS and frequency bands
- Signal quality and consistency monitoring
  - Between GNSS systems and frequency bands
- Navigation data validity checks (eg DHS whitelist)
- Navigation data authentication (Galileo OS-NMA)
- Consistency of PVT solution
  - vs known boundaries and motion
  - vs clock characteristics

Spoofing countermeasures



- Antenna arrays for angle-of-arrival detection
- Power level and spectrum checks
  - Changes over time, between GNSS and frequency bands
- Signal quality and consistency monitoring
  - Between GNSS systems and frequency bands
- Navigation data validity checks (eg DHS whitelist)
- Navigation data authentication (Galileo OS-NMA)
- Consistency of PVT solution
  - vs known boundaries and motion
  - vs clock characteristics
- Redundancy at host system
  - sensor data
  - time information

Conclusion

- GNSS is an excellent source of position, velocity and time, well worth protecting
  - Affordability – free service, easy installation
  - Accuracy – ”atomic clock”-level without atomic clocks
  - Availability – global coverage
- Effective countermeasures cover all stages from antenna to application
- Redundancy is key – multi-GNSS, multi-band
- Threats exist, but also countermeasures evolve

It is an arms race – we are on top of developments

Thank you
for your attention