ANOTHER PLACE, ANOTHER TIME

GPS THREATS AND COUNTERMEASURES IN AUTONOMOUS SYSTEMS

CERTivation

Overview

- Introduction
- Global Navigation Satelite System
- Autonomous Systems
- Threats
- Countermeasures

Introduction

Everybody use it, most of us doesn’t know how it works.

GPS – Navstar – Galileo - Glonas - Beidou - IRNSS

Many names , but where is the difference

Global Navigation Satellite Systems (GNSS)

Stephan Gerling - @ObiWan666

I am older than the internet
Certified as “GCFA, CISSP, MCSE, CCNA, etc.”
Electronic Specialist,
several years German Aviation Army navigation system electronic specialist
More than 32 years a volunteer firefighter in my town
Security Evangelist @ROSEN-Group & @CERTivation in Oil & Gas Industrie
I void warranties

Volunteering
- Geraffel
- IamTheCavalry (maritime security)

Global Navigation Satellite Systems (GNSS)

Global Navigation Satellite Systems (GNSS) - public named GPS

Everybody use it, most of us doesn’t know how it works.

Daily use by most of us (smart Phone/Watch, Car, Plane, etc)

GNSS System overview

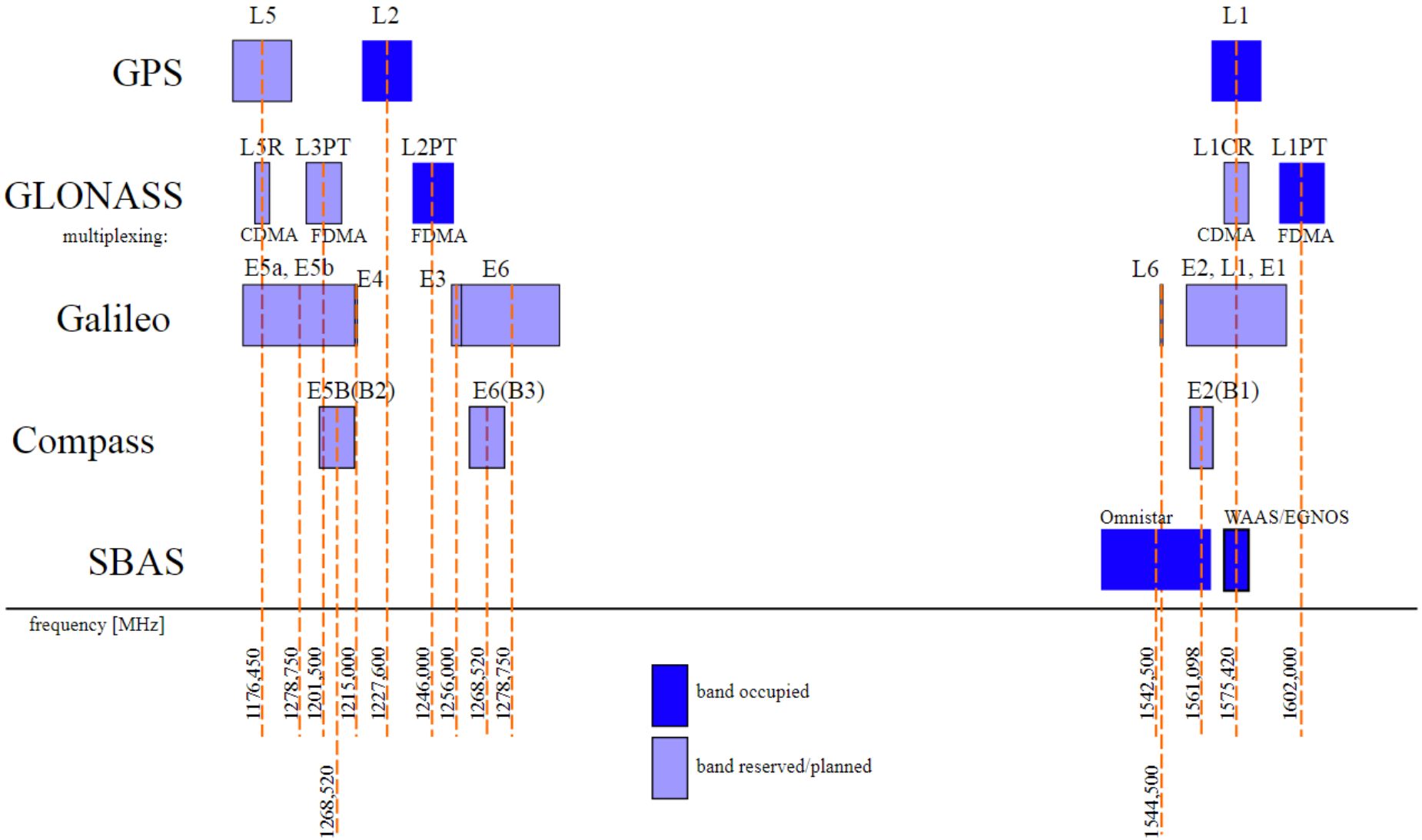
GNSS (**G**lobal **N**avigation **S**atellite **S**ystem)

- NAVSTAR GPS (United Staates of America)
  - **Nav**igational **S**atellite **T**iming **a**nd **R**anging – **G**lobal **P**ositioning **S**ystem
- GLONASS (Russian Föderation)
  - **Glo**balnaya **na**vigatsionnaya **s**putnikovaya **s**istema
- Galileo (Europe Union)
- Beidou (China)
  - Named by a Big Dipper asterism, in Chinese called Běidǒu (北斗)
- IRNSS
  - **I**ndian **R**egional **N**avigation **S**atellite **S**ystem
  - renamed now in NAVIC – **Nav**igation **I**ndian **C**onstellation

GNSS history

	Start of development	first satellite	operational since
Navstar	1973	1978	1990 (fully in 1995)
Glonass	1976	1982	1995
Beidou	1980	2000	2012, 2020 global
Galileo	1999 (2003)	2005	2016 (2020)
IRNSS (NAVIC)	2004	2013	2016

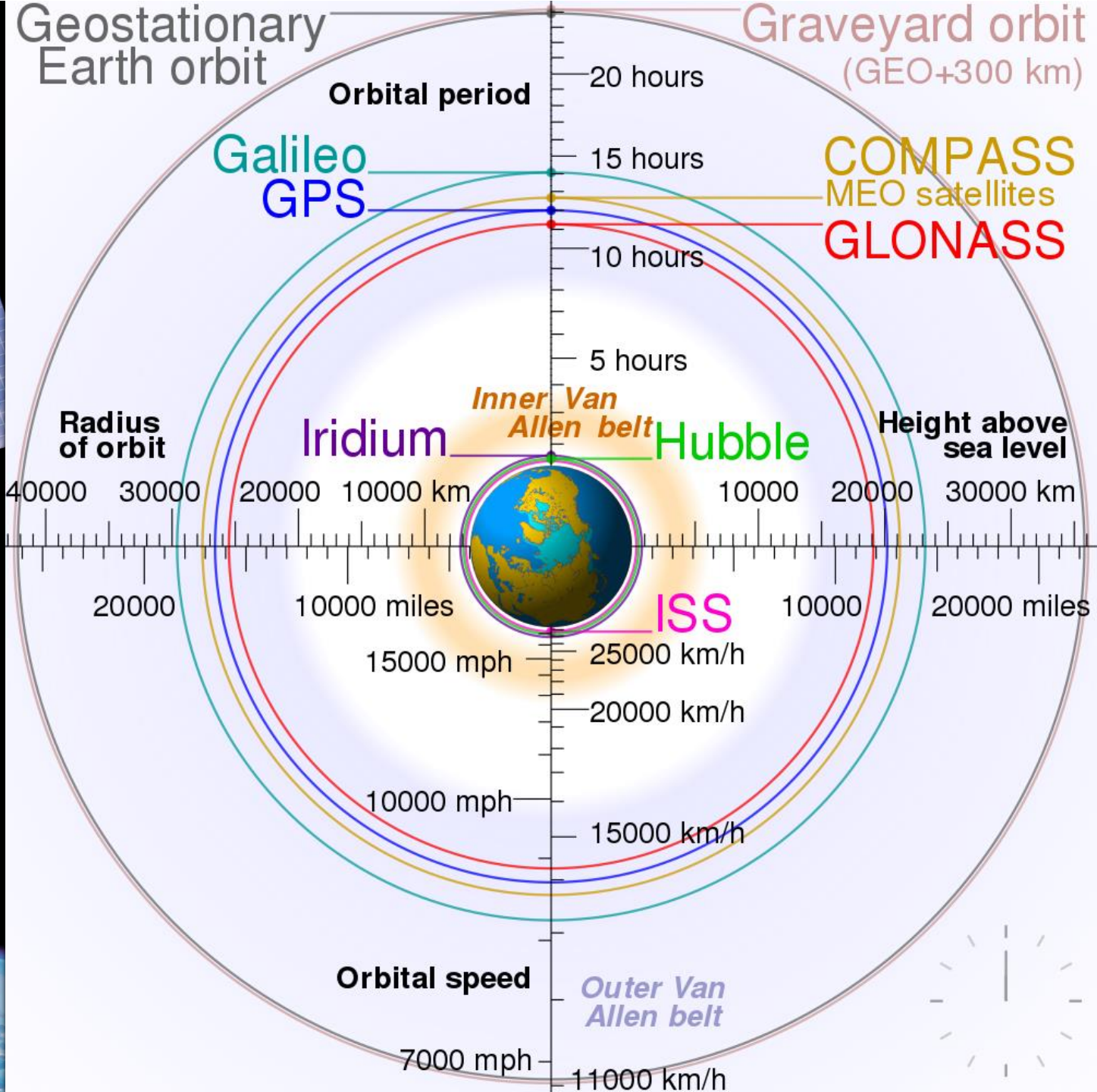
GNSS – frequencys used



https://upload.wikimedia.org/wikipedia/commons/9/9a/Gnss_bandwidth.svg

GNSS – frequencys used

1176.45	MHz	IRNSS, Galileo
1191.795	MHz	Galileo
1207.14	MHz	Galileo
1227.60	MHz	GPS
1246	MHz	Glonas
1278.75	MHz	Galileo
1575.42	MHz	GPS, Beidou, Galileo
1602	MHz	Glonas
1191.795	MHz	Beidou
1268.52	MHz	Beidou
2492.028	MHz	IRNSS, Beidou (Test frequency)


Geostationary Earth orbit
Graveyard orbit (GEO+300 km)
Orbital period
20 hours
15 hours
10 hours
5 hours
Galileo
GPS
COMPASS
MEO satellites
GLONASS
Inner Van Allen belt
Iridium
Hubble
Radius of orbit
Height above sea level
40000 30000 20000 10000 km
10000 20000 30000 km
20000 10000 miles
10000 20000 miles
ISS
15000 mph
25000 km/h
20000 km/h
10000 mph
15000 km/h
Orbital speed
Outer Van Allen belt
7000 mph
11000 km/h

Autonomous Systems

Autonomous systems rely on insecure positioning system

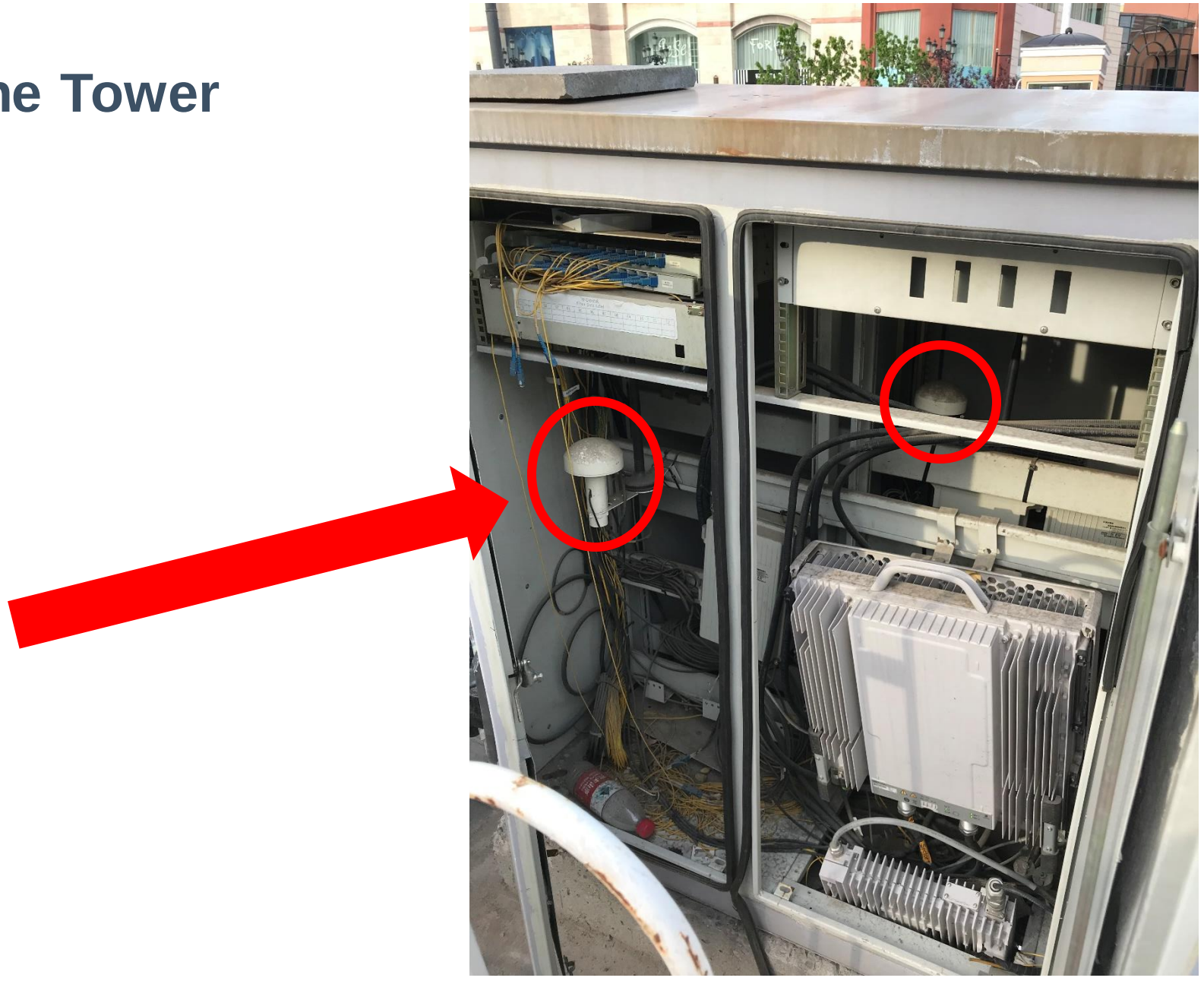
- Self driving Cars, Bus, Truck, Trains
- Autonoumous Ships – Cargo Vessels, Sailing Yachts, etc.

But also other Industries uses GNSS as synchronized Timing Source

- Finance - real Time Trading, Stock exchange…..
- Power Grids, Industrial Plants, Pipeline Operators, Cellphone Towers
- Many others

Just to give a few exanmples

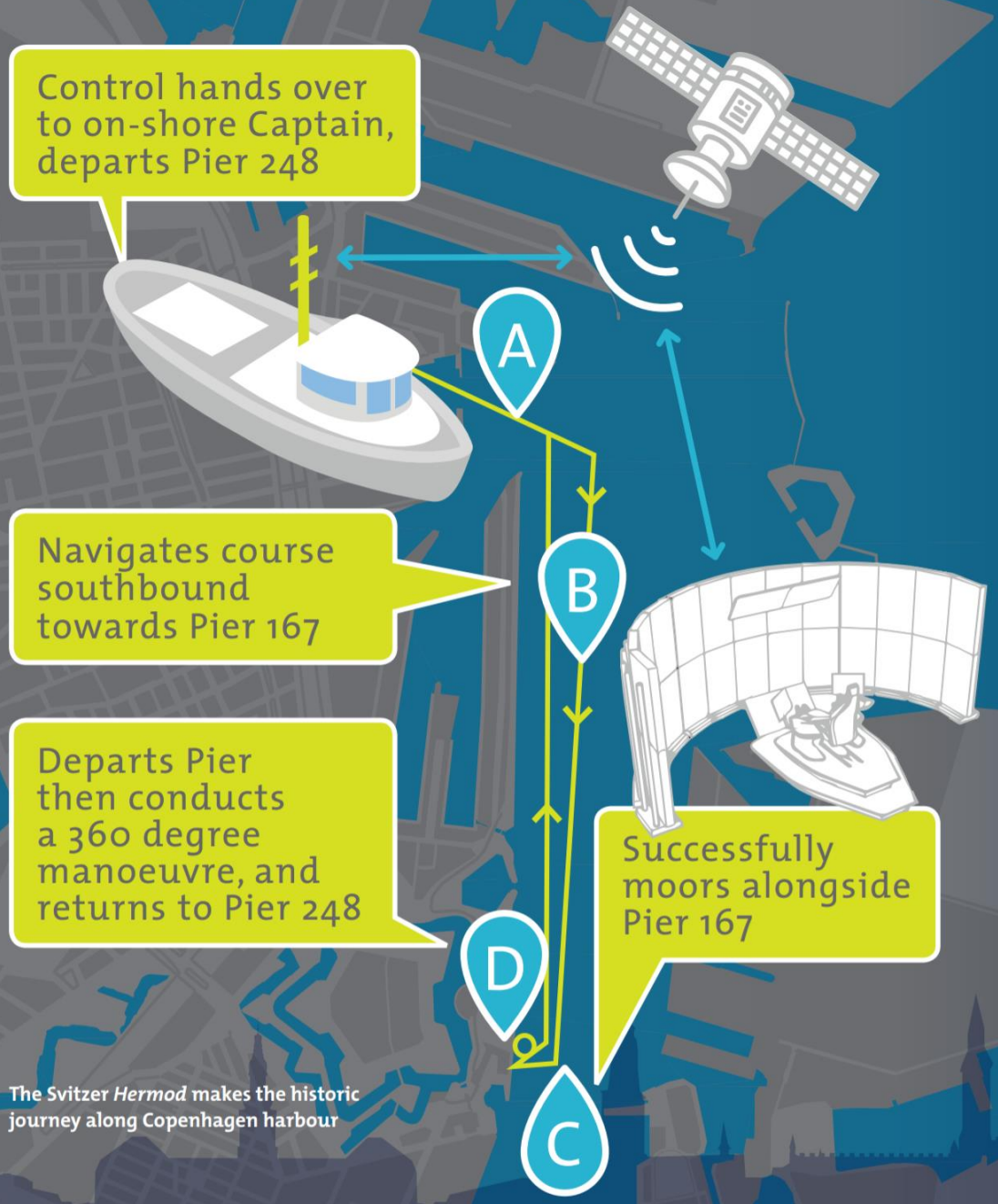
Cell Phone Tower



Autonomous Trains

Source: Vodafone GmbH

The world's first remote control commercial vessel



The Svitzer *Hermod* makes the historic journey along Copenhagen harbour

Key facts

Rolls-Royce and Svitzer demonstrate the world's first remote controlled commercial vessel ● Test took place in Copenhagen harbour ● The 28 metre Svitzer *Hermod* was controlled by a Captain from shore ● It successfully demonstrated vessel navigation, situational awareness, remote control and communications systems ● Rolls-Royce Remote Operations Centre features state-of-the-art control ● Combination of Radar, Lidar and camera technology ensures Captain's awareness of surroundings

The tech

On board sensors to give Captain full awareness of surroundings

Sensors covering Radar, Lidar, camera and audio

State-of-the-art Remote Operations Centre on shore

Rolls-Rolls Dynamic Positioning systems control position of the vessel via satellite

The test

400+ individual validations met

42 individual safety requirements met

Passed 61 mandatory cyber security tests

Completed 16 hours of remote control operation and overseen by Lloyd's Register

The vessel

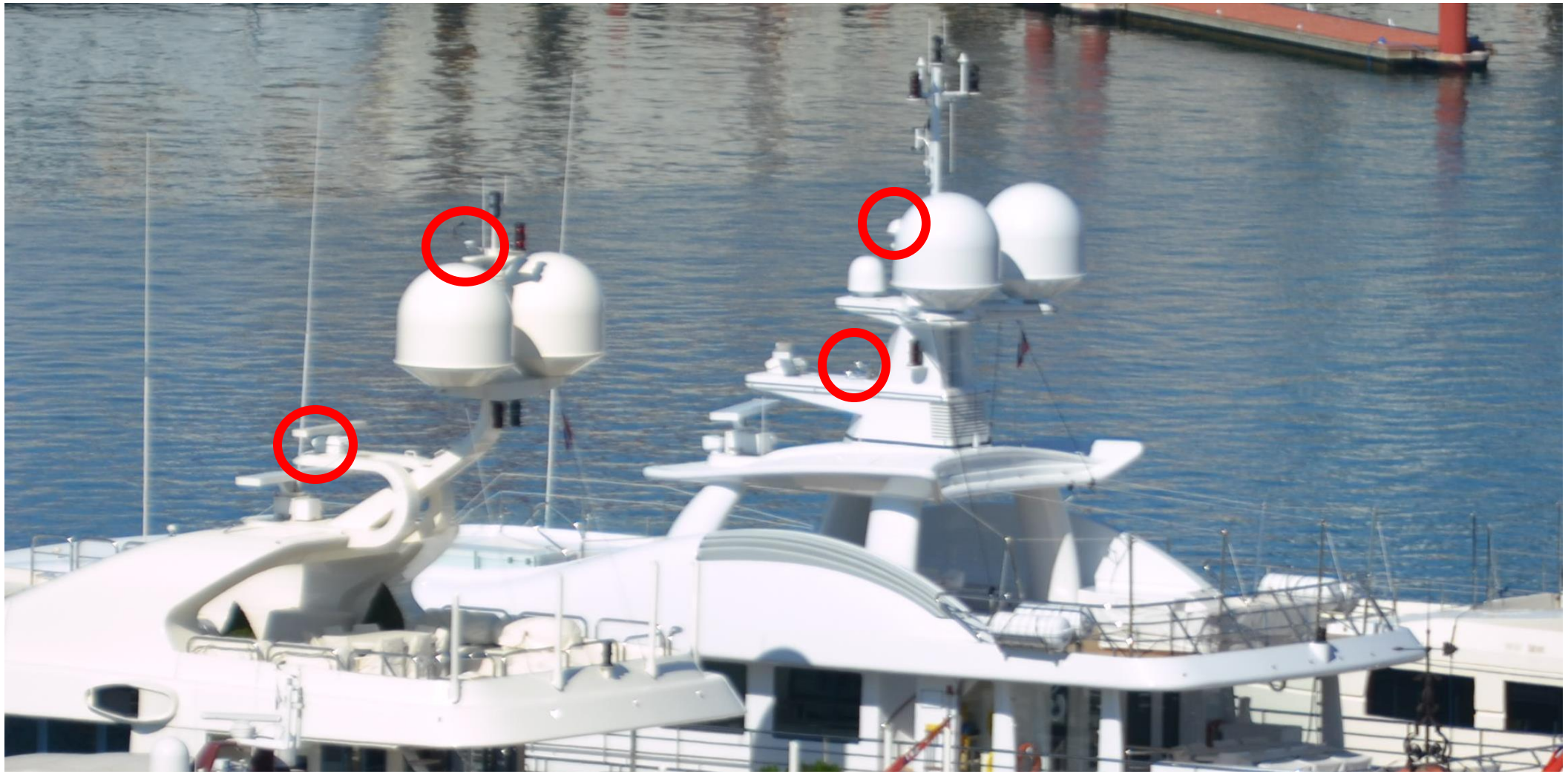
28 metre tug Svitzer *Hermod*

Built in 2016

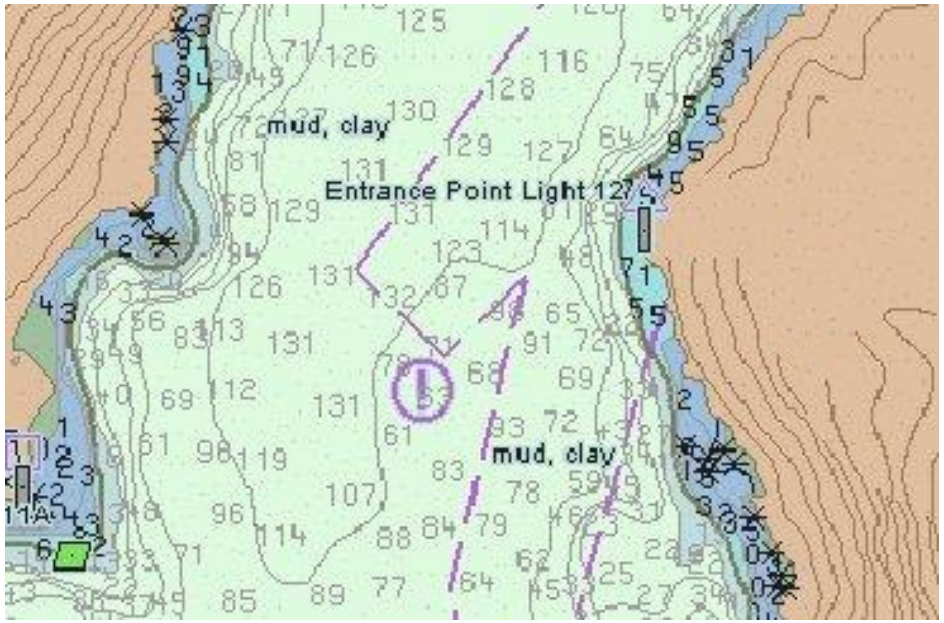
2 x MTU 16V4000 M63 diesel engines

Rolls-Royce

GPS on Yachts



Electronic Maps on Ships



In past, Nautical Charts required

Regulation changed

2 or more independent GPS systems required for

- Electronic Navigational Charts (ENC)
- or Digital Nautical Charts (DNC)

To Navigate with ECDIS (electronic Chart Display Information System)

Independend ! - In case of the device or GNSS?

Services on Yachts relaying on GPS

GPS Sensor receiving position

- Send it onto the internal “CAN” BUS (NMEA2000 BUS)

Services using this Position information

- AIS (automatic identification system)

AIS is therefore the source for

- VTS (Vessel Traffic Service)
- ECDIS (electronic chart display and information service)

Is your Smartphone supporting Galileo?

U can lookup supported devices under

https://www.usegalileo.eu/EN/

- Maritime
- Road
- Train
- Air
- Mobile
- IOT
- Etc.

GNSS or GPS threats

GNSS threats

3 Scenarios are possible

- jamming
- Spoofing
- DoS

complexibility:

Jamming = quite simple

Spoofing = complex – requires special hardware

DoS = very complex, requires access to the Groundstations

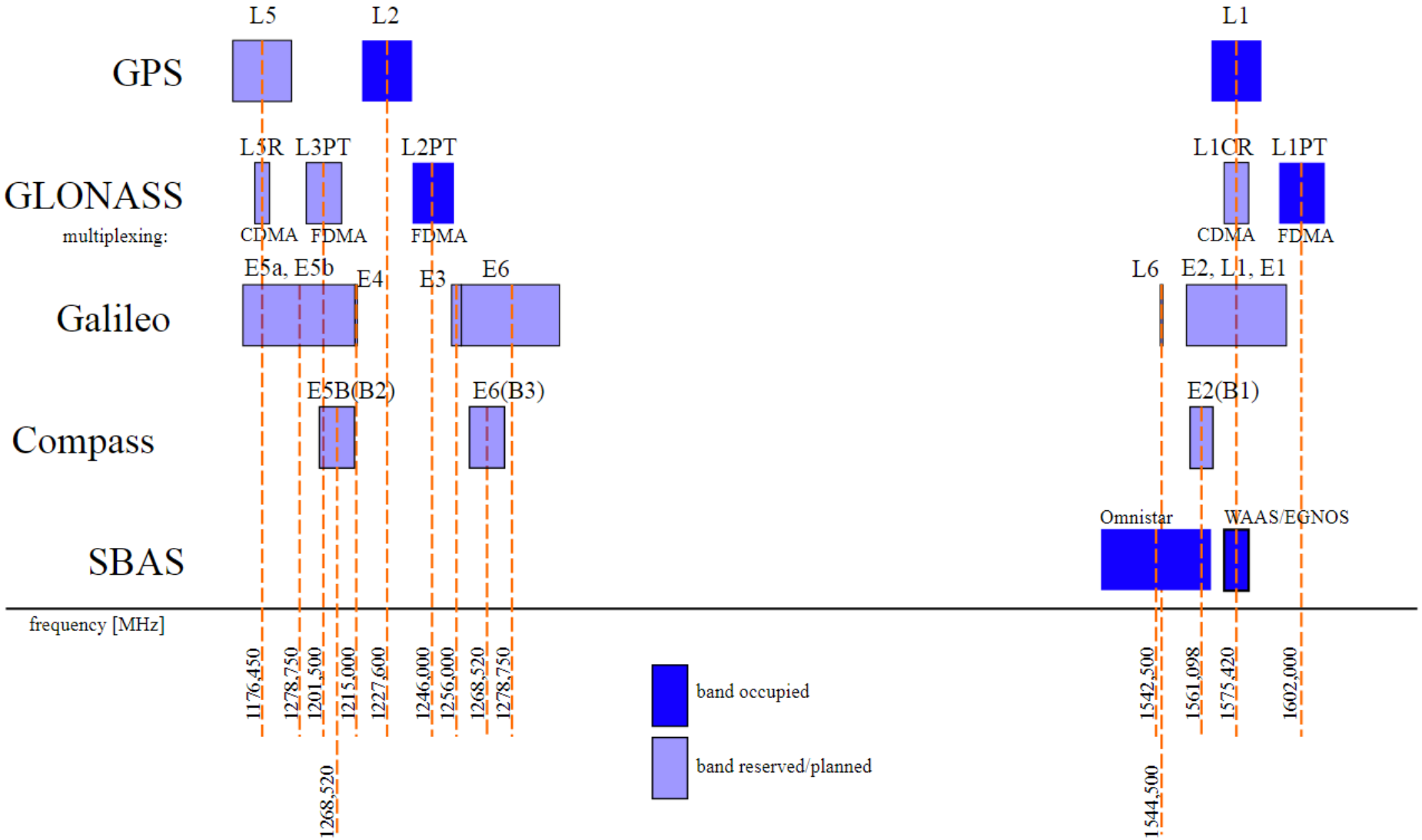
GPS - Jamming

Eastern Pacific reports more and more GPS anomalies

- Juni, week 25 – more than 20 reports – north east black see
- NATO Troops maneuver at same time there
- Sept. Norway reports anomalies in a height >2000ft
- https://rntfnd.org/wp-content/uploads/Norway-Comms-Auth-Report-GPS-Jamming-Sept-2017.pdf

- US Navy teaching again offline Navigation with Sixtant

GPS – frequencys used



https://upload.wikimedia.org/wikipedia/commons/9/9a/Gnss_bandwidth.svg

GNSS jamming

Generating frequency noise on the L1 Band

1227.60	MHz	GPS
1575.42	MHz	GPS
1246	MHz	Glonas
1602	MHz	Glonas
1176.45	MHz	IRNSS
2492.028	MHz	IRNSS

GNSS jamming

1575.42 MHz	Beidou,
1191.795 MHz	Beidou
1268.52 MHz	Beidou
2492.028 MHz	Beidou
1176.45 MHz	Galileo
1191.795 MHz	Galileo
1207.14 MHz	Galileo
1278.75 MHz	Galileo
1575.42 MHz	Galileo

GPS jammers sold online

USB GPS Jammer | Blocks GPS L1 & L2 | Coverage up to 10 meters | Power by 5V USB

$79.00

1 Review(s)

Mini GPS Jammer, Anti tracking device

$79.00

6 Review(s)

Ligther Type GPS Car Jammer to Protect Your Car

$79.00

7 Review(s)

https://www.cell-jammers.com/gps-jammers

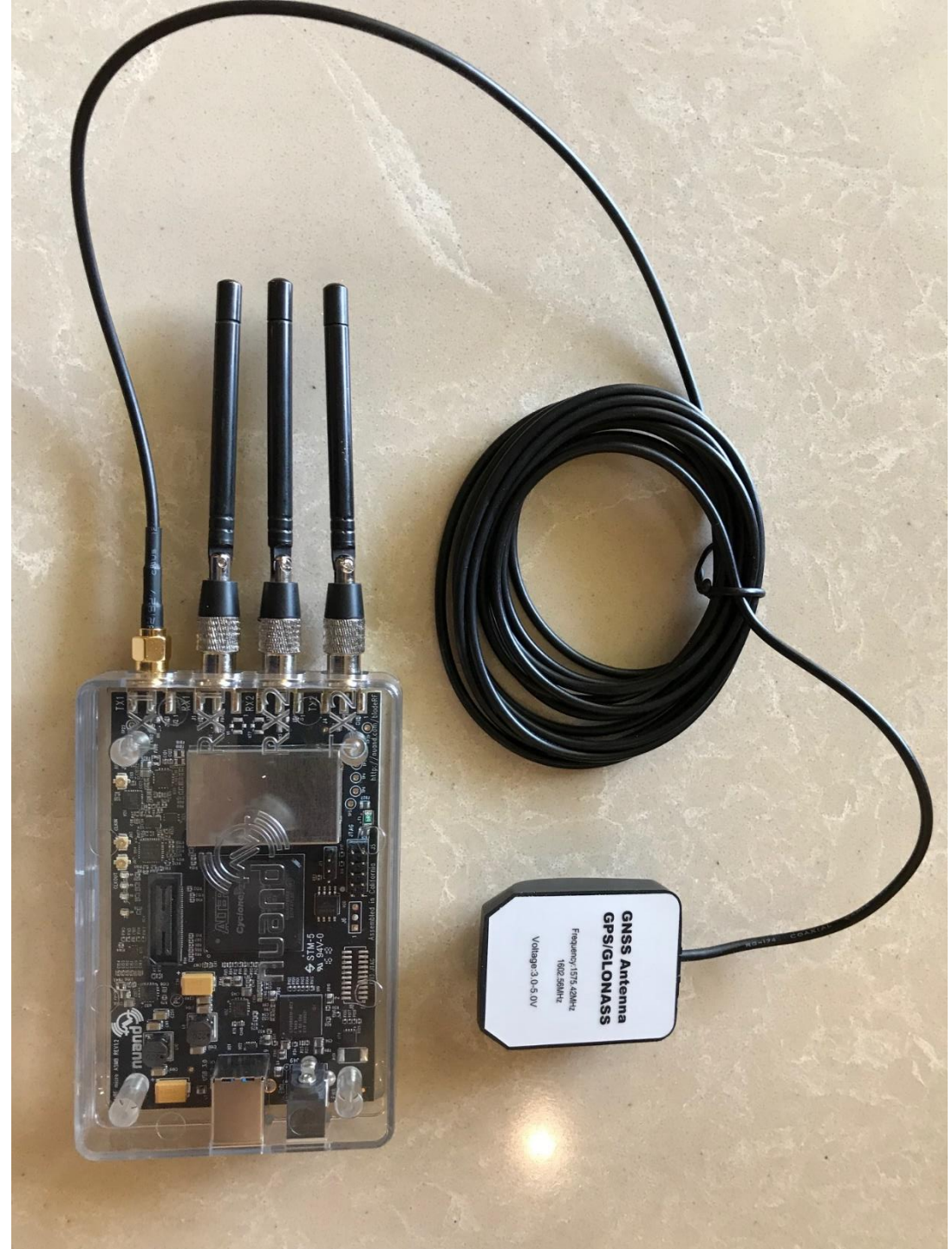
GPS spoofing

Spoofing GPS signal is becoming easy

Specialized Hardware available for it.

For example Labsat GNSS Simulator
https://www.labsat.co.uk/index.php/de/produkte/labsat-3-de


HackRF One
GREAT SCOTT GADGETS
GNSS Antenna
GPS/GLONASS
Frequency:1575.42MHz
1602.56MHz
Voltage:3.0-5.0V
CLKIN
CLKOUT


GNSS Antenna
GPS/GLONASS
Frequency:1575.42MHz
1602.56MHz
Voltage:3.0-5.0V

GPS spoofing DIY

Advice:

Don’t mess with GPS signals
Use a faraday cage
or forensic bag for test

GPS spoofing DIY

Software needed

GPS-SDR-SIM

- GPS-SDR-SIM generates GPS baseband signal data streams, which can be converted to RF using software-defined radio (SDR) platforms, such as ADALM-Pluto, bladeRF, HackRF, and USRP.

https://github.com/osqzss/gps-sdr-sim

GPS spoofing DIY

What is needed to spoof GPS signals

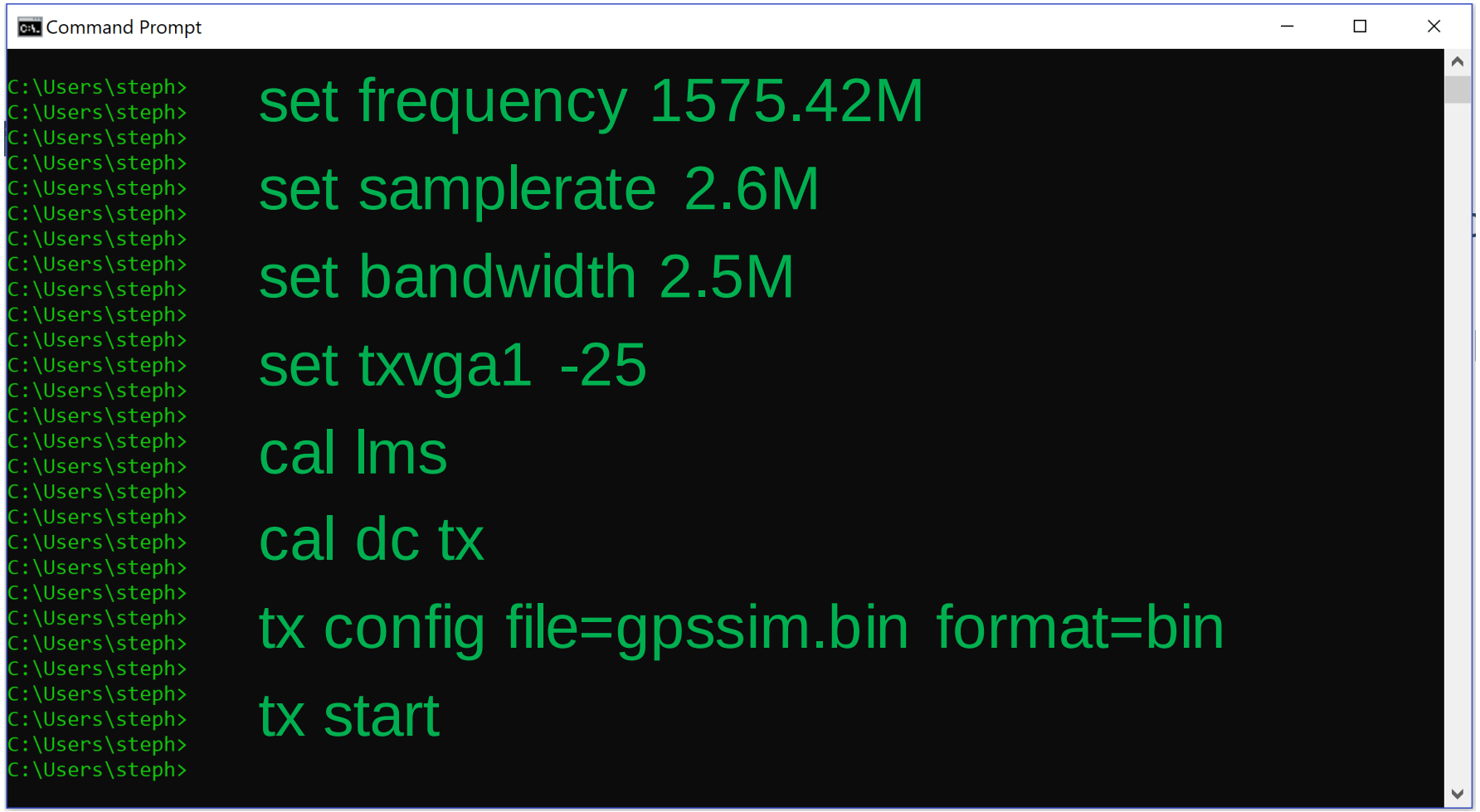
Daily GPS broadcast ephemeris file (ftp://cddis.gsfc.nasa.gov/gnss/data/daily)

generate the simulated pseudorange with gps-sdr-sim

CSV file with positions that you want to simulate (or static position)
Generate the simulation file
Transmitting via SDR – device (HackRF or bladeRF)

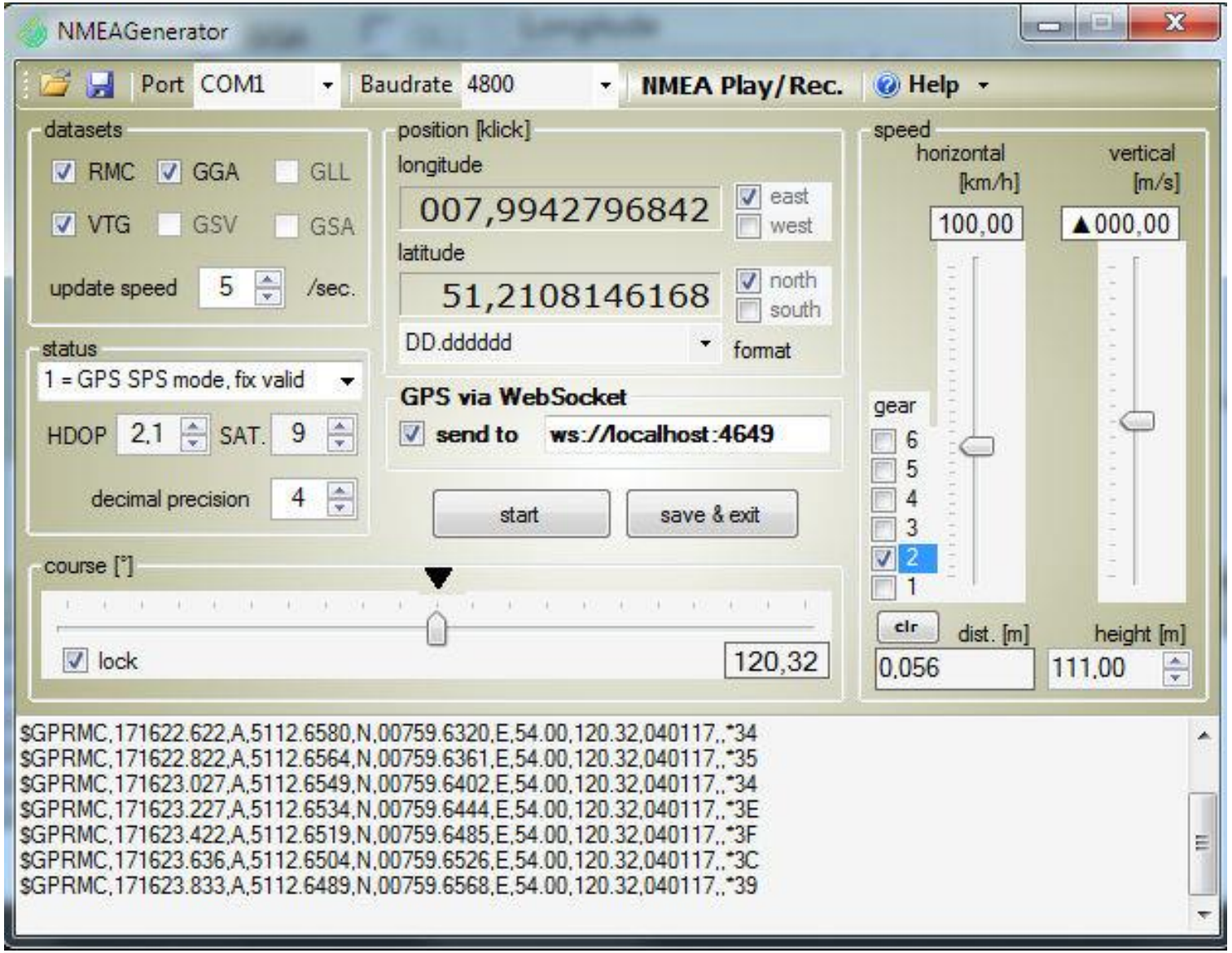
GPS spoofing DIY

Transmitting in bladeRF-cli



Attacking the NMEA Bus

With physical access to NMEA network



http://www.atlsoft.de/gps-simulator/

Galileo outage (1 week)

On 11. July Galileo GNSS system was going offline.

After 11 days back to “initial Service” (See NAGU messages)

Outage https://www.gsc-europa.eu/notice-advisory-to-galileo-users-nagu-2019026

Back to operation https://www.gsc-europa.eu/notice-advisory-to-galileo-users-nagu-2019028

Not official Root cause:

Atomic clocks at Ground control in Fucino (IT) had some issues

Same time Backup system in Germany was down for Maintenance

Coordination to recovery took to long

Synchronizing of clock signal to Satelit stopped

Each satellite stopped sending

But SAR service was not affected

GPS countermeasures

What can we do?

- Hardware approach
- Software solutions

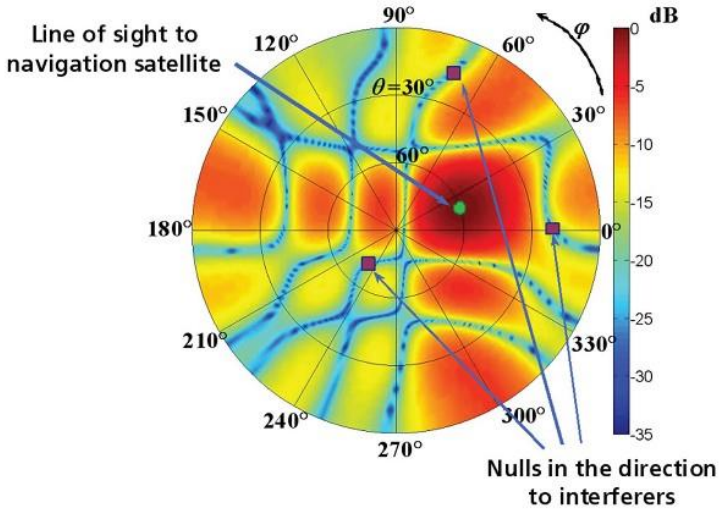
GPS countermeasures

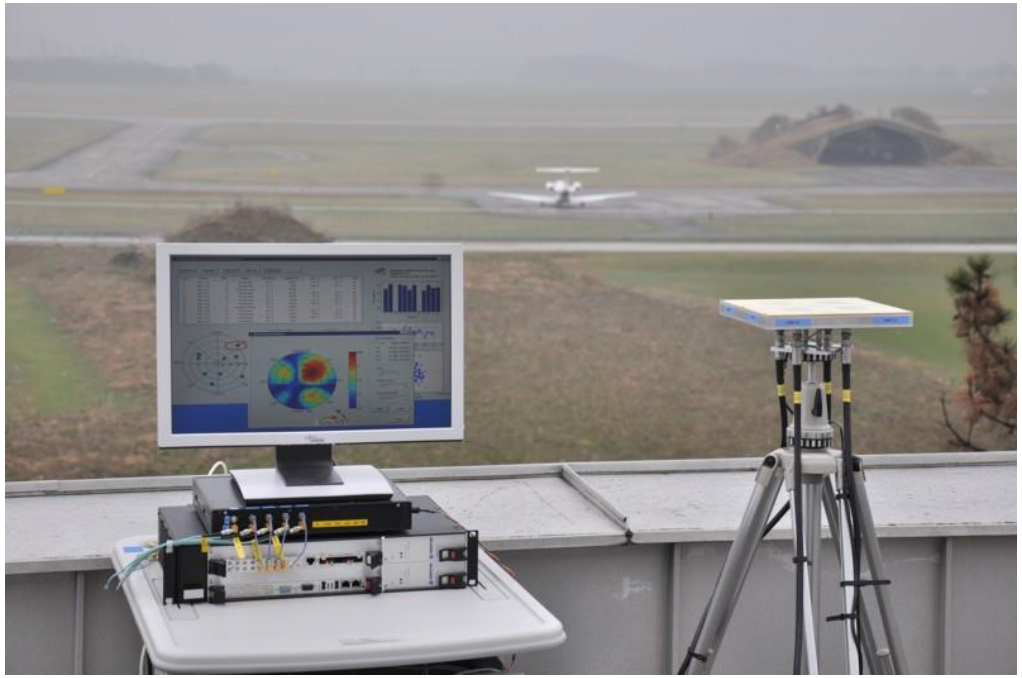
- Signal strength change detection
- Plausible checks on time jumps
- Pseudo Antenna (wiggling Antenna is virtual 2 antenna)
- Compare 2 or all available GNSS positions

Securing GPS?

Research Project – „Galant“ by DLR – Institute of communications and navigation

- 2x2 active antenna array
- Beamforming & array processing

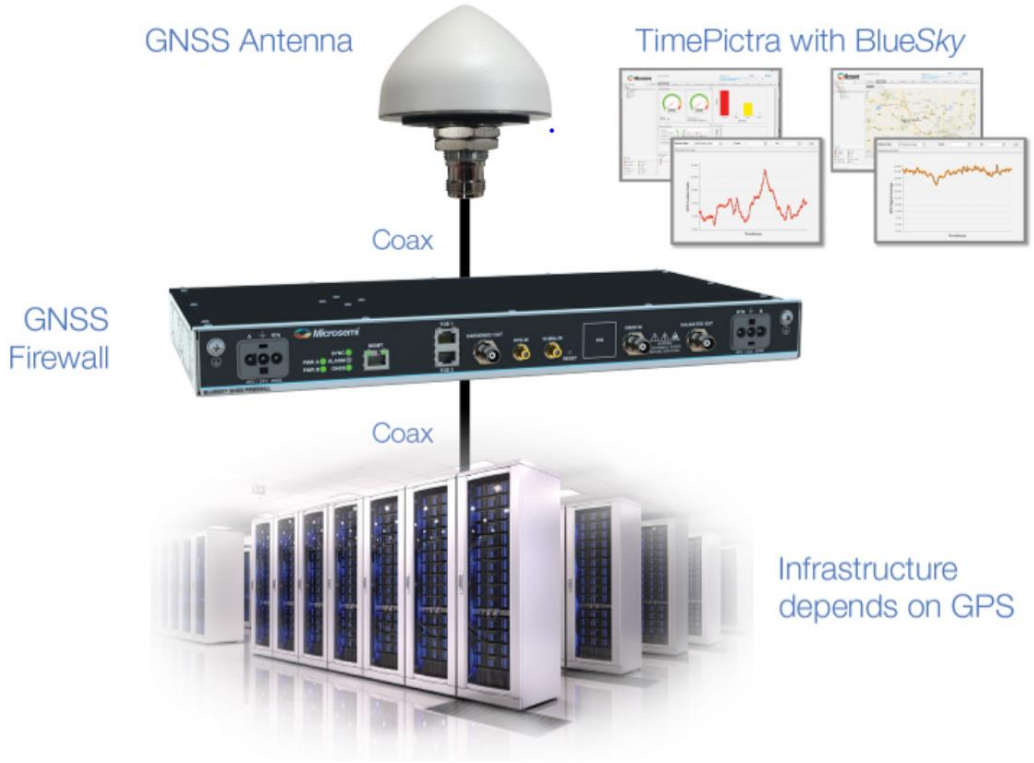




http://www.dlr.de/kn/en/desktopdefault.aspx/tabid-4306/6938_read-9224/

Securing GPS?

Just by an GNSS Firewall



Protects GPS Systems

against spoofing and jamming threats

software engine analyzes the GPS signal.

GPS signal data is received and evaluated from each satellite to ensure compliance along with analyzing received signal characteristics.

https://www.microsemi.com/product-directory/gps-instruments/4398-bluesky-gps-firewall

conclusion

- GPS attacks occours often
- Mostly jamming
- First products are available to protect
- Spoofing is not that easy, but possible

Linkedin: Stephan Gerling
Twitter: @ObiWan666
E-Mail: SGerling@ROSEN-Group.com

THANK YOU FOR JOINING THIS PRESENTATION.

www.certivation.com

CERTivation