ITSF 2021 – Brighton, UK

Turning the Tables on the Spoofers

- “self-spoofing” systems supplying secure signals to augment existing PNT receivers.

Christian Farrow B.Sc. (Hons) MinstP MIET
Technical Services Manager @ChronosTechno

Chronos: Sync & Timing Expertise since 1986

- Professional Services
- Training, Install/Commission & Support
- Network Sync Audits – Time & Timing
- Network Design & Test
- Consultancy

- ITU Standards Committee (SG15/Q13)
- Steering Groups – ITSF, WSTS & RIN

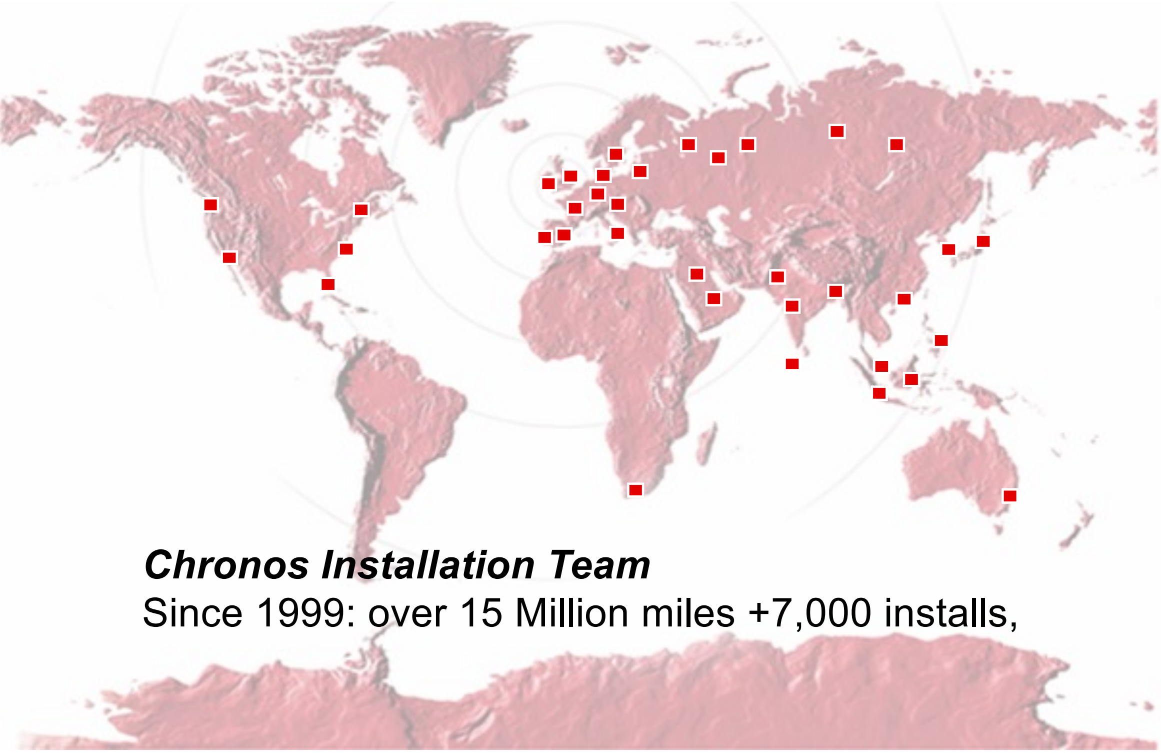
- R&D, product development
- Expert Advisory Groups (Blackett, RAEng)

- Resilient Synchronisation & Timing Solutions
- GNSS Vulnerability & Mitigation Solutions

- Markets
  - Telecom
  - Power
  - Financial Services
  - Defence & Security
  - Law Enforcement
  - Broadcast

Chronos Technology

- Global reach – installations + support
- ***Extensive experience of how GNSS timing systems behave in the real world***

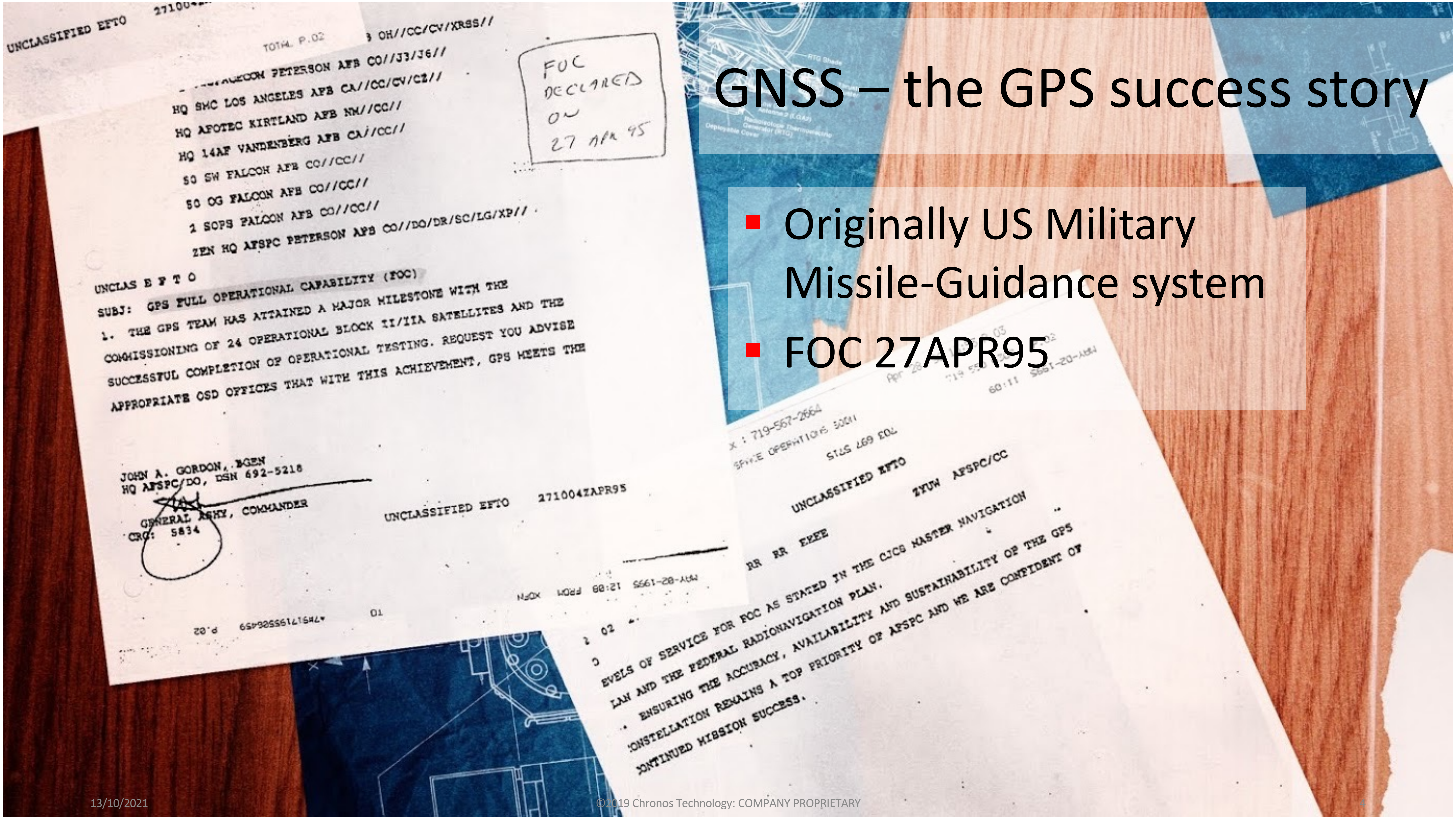


Chronos Installation Team

Since 1999: over 15 Million miles +7,000 installs,

GNSS – the GPS success story

- Originally US Military Missile-Guidance system
- FOC 27APR95



UNCLASSIFIED EFTO 27100

TOTAL P.02

OH//CC/CV/XRSS//

PETERSON AFB CO//J3/J6//
HQ SMC LOS ANGELES AFB CA//CC/CV/CZ//
HQ AFOTEC KIRTLAND AFB NM//CC//
HQ 14AF VANDENBERG AFB CA//CC//
50 SW FALCON AFB CO//CC//
50 OG FALCON AFB CO//CC//
1 SOPS FALCON AFB CO//CC//
ZEN HQ AFSPC PETERSON AFB CO//DO/DR/SC/LG/XP//

FOC DECLARED ON 27 APR 95

UNCLAS E F T O

SUBJ: GPS FULL OPERATIONAL CAPABILITY (FOC)

1. THE GPS TEAM HAS ATTAINED A MAJOR MILESTONE WITH THE COMMISSIONING OF 24 OPERATIONAL BLOCK II/IIA SATELLITES AND THE SUCCESSFUL COMPLETION OF OPERATIONAL TESTING. REQUEST YOU ADVISE APPROPRIATE OSD OFFICES THAT WITH THIS ACHIEVEMENT, GPS MEETS THE

JOHN A. GORDON, BGEN
HQ AFSPC/DO, DSN 692-5218

GENERAL ASHY, COMMANDER
CRC: 5834

UNCLASSIFIED EFTO 271004ZAPR95

x : 719-567-2664
SPACE OPERATIONS

UNCLASSIFIED EFTO

RR RR EEEE ZYUW AFSPC/CC

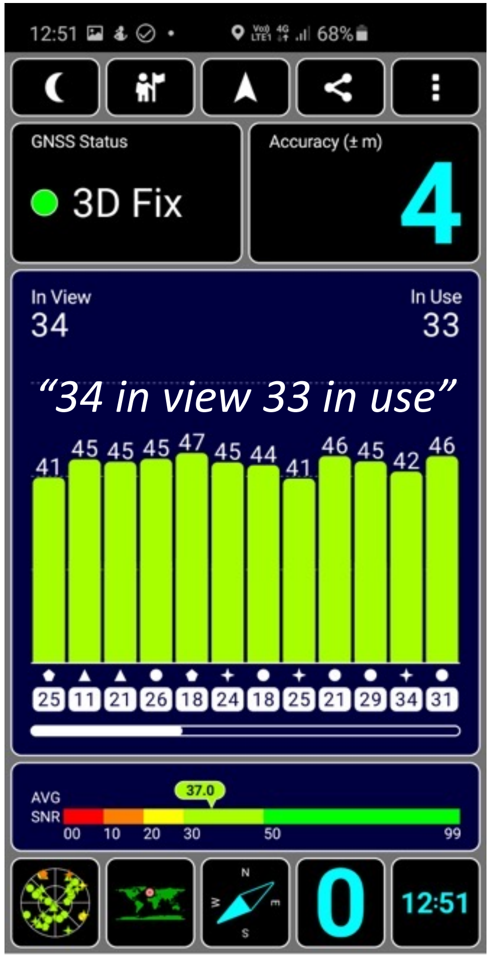
EVELS OF SERVICE FOR FOC AS STATED IN THE CJCS MASTER NAVIGATION LAN AND THE FEDERAL RADIONAVIGATION PLAN.

ENSURING THE ACCURACY, AVAILABILITY AND SUSTAINABILITY OF THE GPS ONSTELLATION REMAINS A TOP PRIORITY OF AFSPC AND WE ARE CONFIDENT OF ONTINUED MISSION SUCCESS.

Mid-1990s

- Civilian applications emerge:
  - Telecom Frequency reference
  - Handheld personal Nav receivers

The commoditisation of GNSS



12:51 68%

GNSS Status: 3D Fix

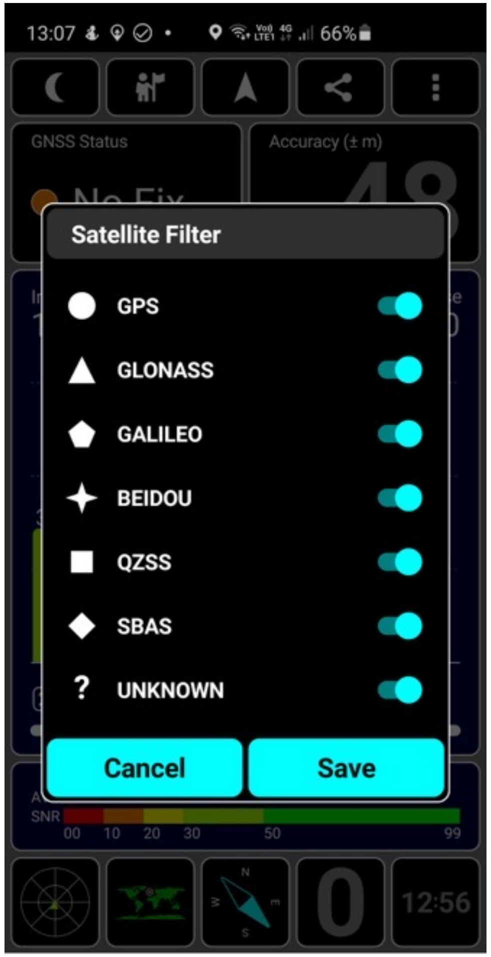
Accuracy (± m): 4

In View: 34

In Use: 33

“34 in view 33 in use”

- Approx. 60 million smartphones in use in the UK (2019)
- 2019 Android handset with multi-constellation receiver sees:
  - GPS, GLONASS, GALILEO, BEIDOU, SBAS (+QZSS)
- Mass use of GNSS for positioning has spread the knowledge of location spoofing to a much wider audience
  - *From app level to actual GNSS radio signal spoofing*



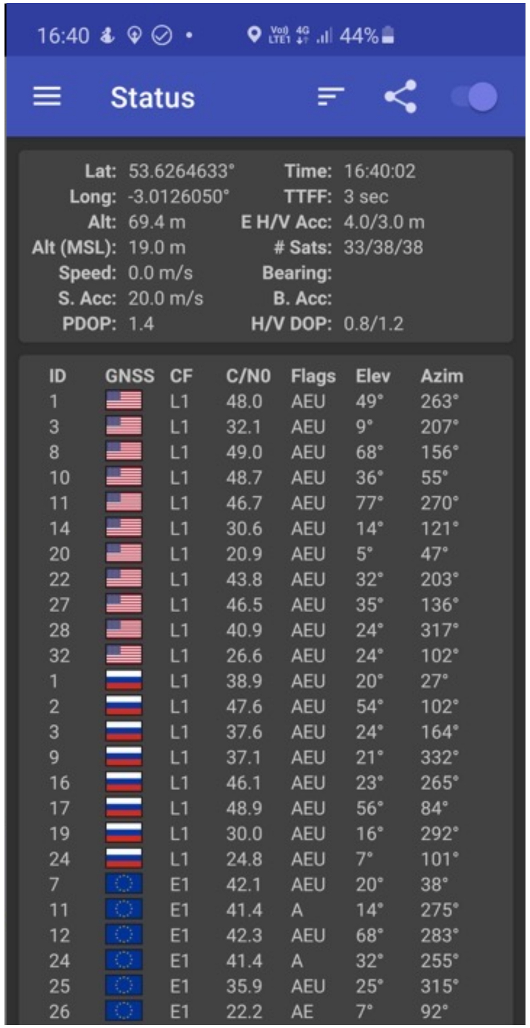
13:07 66%

Satellite Filter

- ○ GPS: on
- ▲ GLONASS: on
- ⬟ GALILEO: on
- ✦ BEIDOU: on
- ■ QZSS: on
- ◆ SBAS: on
- ? UNKNOWN: on

1999 vs. 2019

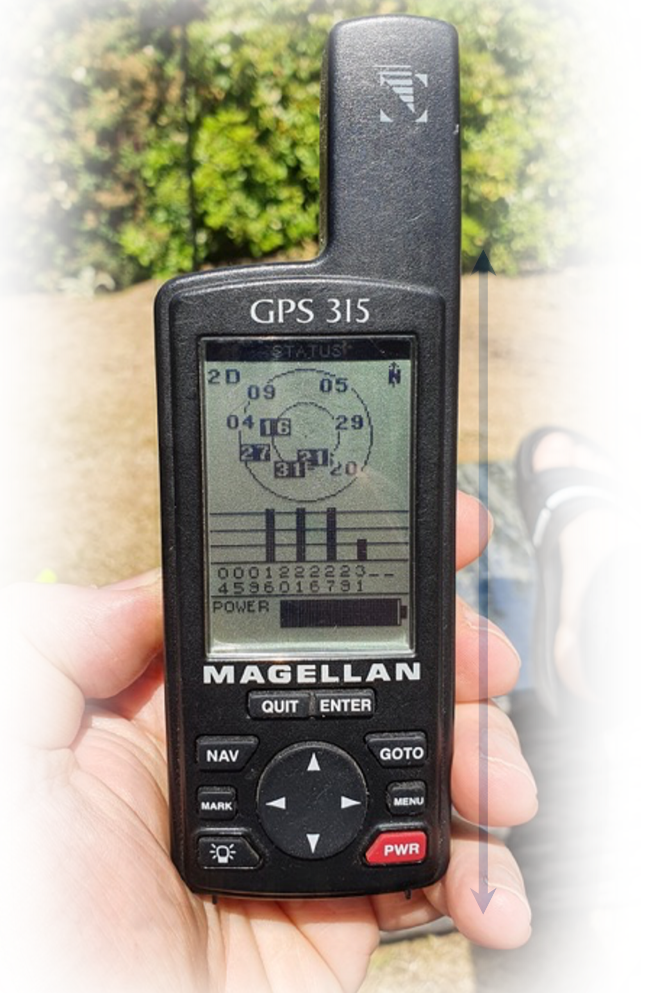
- 1999
  - Handheld GPS only “12 channel” (custom ASIC)
  - TTFF ~ several minutes
- 2019
  - Android Samsung Galaxy S10+ (Broadcom BCM47752KLB1G)
  - TTFF 3s

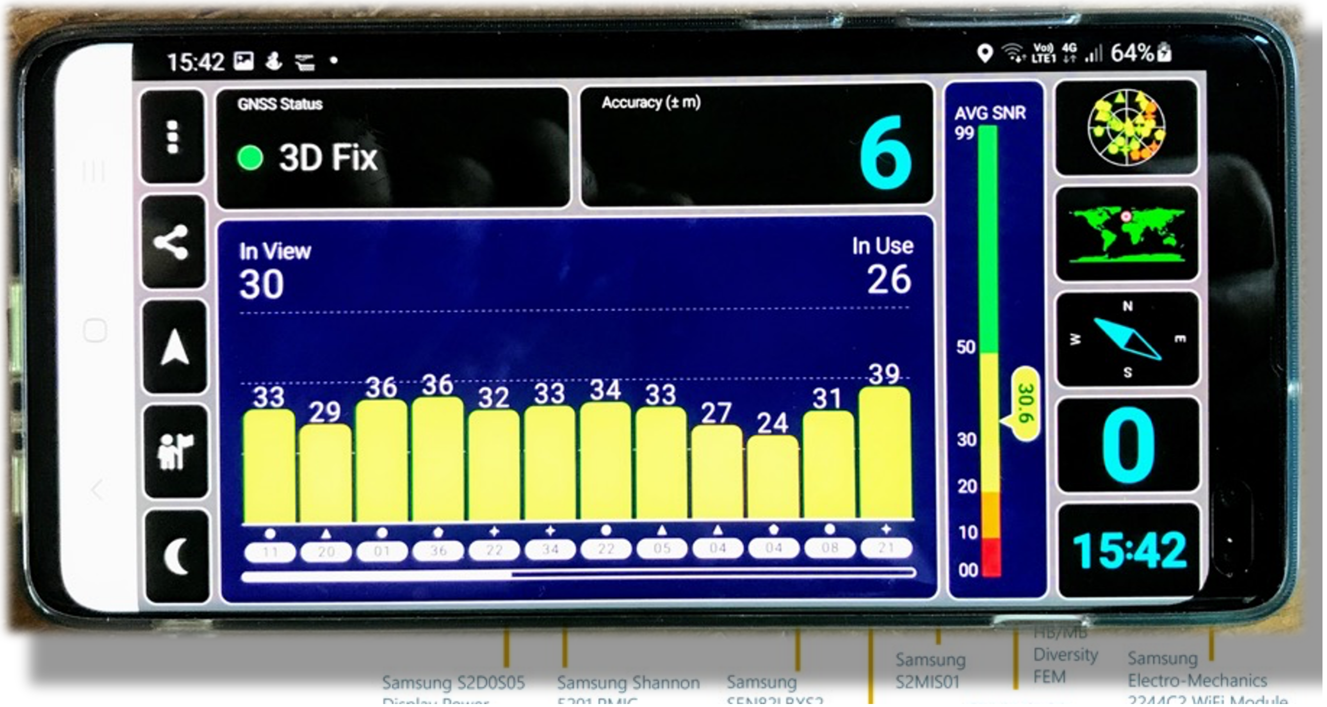


Lat:	53.6264633°	Time:	16:40:02
Long:	-3.0126050°	TTFF:	3 sec
Alt:	69.4 m	E H/V Acc:	4.0/3.0 m
Alt (MSL):	19.0 m	# Sats:	33/38/38
Speed:	0.0 m/s	Bearing:	
S. Acc:	20.0 m/s	B. Acc:	
PDOP:	1.4	H/V DOP:	0.8/1.2

ID	GNSS	CF	C/N0	Flags	Elev	Azim
1	🇺🇸	L1	48.0	AEU	49°	263°
3	🇺🇸	L1	32.1	AEU	9°	207°
8	🇺🇸	L1	49.0	AEU	68°	156°
10	🇺🇸	L1	48.7	AEU	36°	55°
11	🇺🇸	L1	46.7	AEU	77°	270°
14	🇺🇸	L1	30.6	AEU	14°	121°
20	🇺🇸	L1	20.9	AEU	5°	47°
22	🇺🇸	L1	43.8	AEU	32°	203°
27	🇺🇸	L1	46.5	AEU	35°	136°
28	🇺🇸	L1	40.9	AEU	24°	317°
32	🇺🇸	L1	26.6	AEU	24°	102°
1	🇷🇺	L1	38.9	AEU	20°	27°
2	🇷🇺	L1	47.6	AEU	54°	102°
3	🇷🇺	L1	37.6	AEU	24°	164°
9	🇷🇺	L1	37.1	AEU	21°	332°
16	🇷🇺	L1	46.1	AEU	23°	265°
17	🇷🇺	L1	48.9	AEU	56°	84°
19	🇷🇺	L1	30.0	AEU	16°	292°
24	🇷🇺	L1	24.8	AEU	7°	101°
7	🇪🇺	E1	42.1	AEU	20°	38°
11	🇪🇺	E1	41.4	A	14°	275°
12	🇪🇺	E1	42.3	AEU	68°	283°
24	🇪🇺	E1	41.4	A	32°	255°
25	🇪🇺	E1	35.9	AEU	25°	315°
26	🇪🇺	E1	22.2	AE	7°	92°

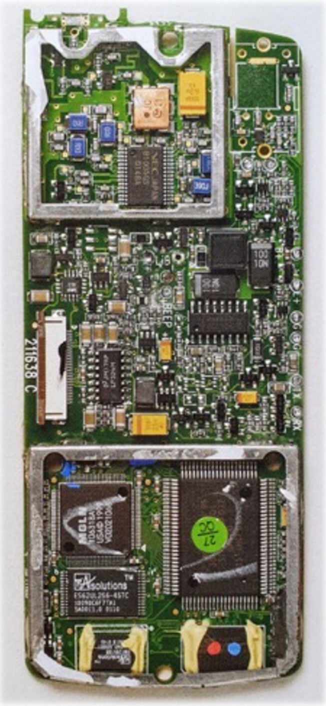
1999 vs. 2019


GPS 315
STATUS
2D
09
05
04
16
29
27
31
21
20
0001222223
4596016781
POWER
MAGELLAN
QUIT
ENTER
NAV
GOTO
MARK
MENU
PWR


15:42
64%
GNSS Status
3D Fix
Accuracy (± m)
6
In View
30
In Use
26
33
29
36
36
32
33
34
33
27
24
31
39
11
20
01
36
22
34
22
05
04
04
08
21
AVG SNR
99
50
30
20
10
00
30.6
N
W
E
S
0
15:42
Samsung S2D0S05
Display Power
Samsung Shannon
5201 PMIC
Samsung
S2MIS01
HB/MB
Diversity
FEM
Samsung
Electro-Mechanics
2244C2 WiFi Module

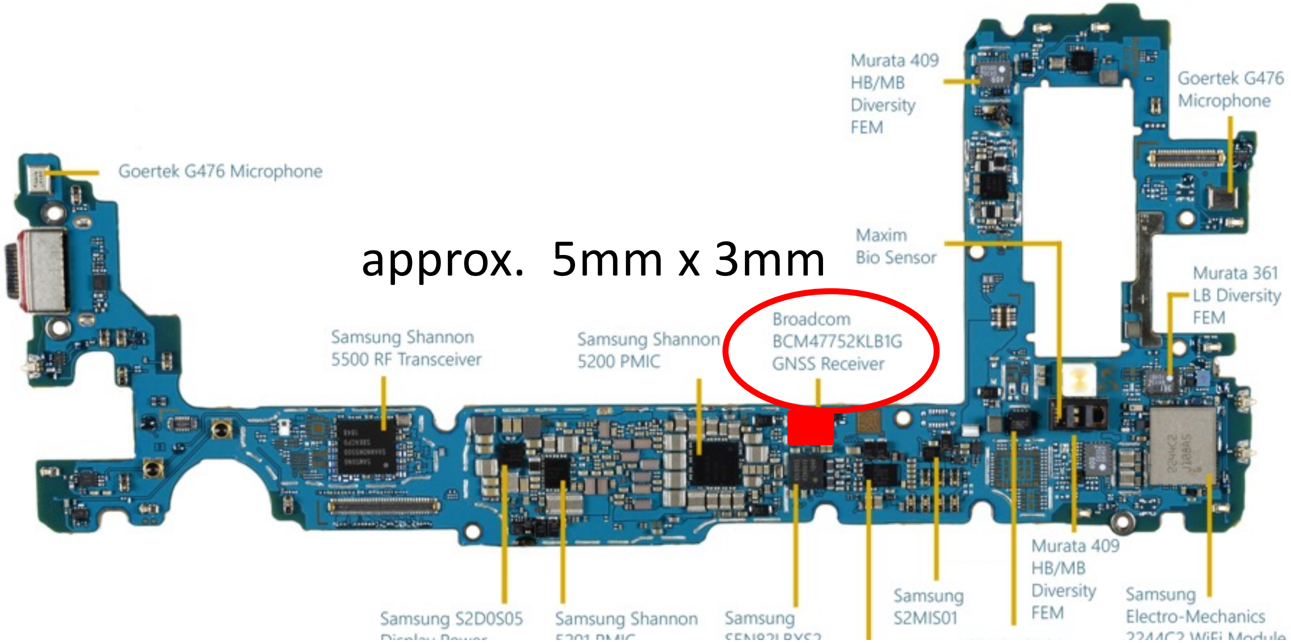
1999 vs. 2019

- GPS315 PCB vs. BCM47752KLB1G (1/500th area)



approx.
11.5cm
(4.5”)

approx. 16cm (6.25”)


Murata 409 HB/MB Diversity FEM
Goertek G476 Microphone
Goertek G476 Microphone
Maxim Bio Sensor
Murata 361 LB Diversity FEM
Broadcom BCM47752KLB1G GNSS Receiver
Samsung Shannon 5500 RF Transceiver
Samsung Shannon 5200 PMIC
Samsung S2D0S05 Display Power
Samsung Shannon 5201 PMIC
Samsung
Samsung S2MIS01
Murata 409 HB/MB Diversity FEM
Samsung Electro-Mechanics 2244C2 WiFi Module

approx. 5mm x 3mm

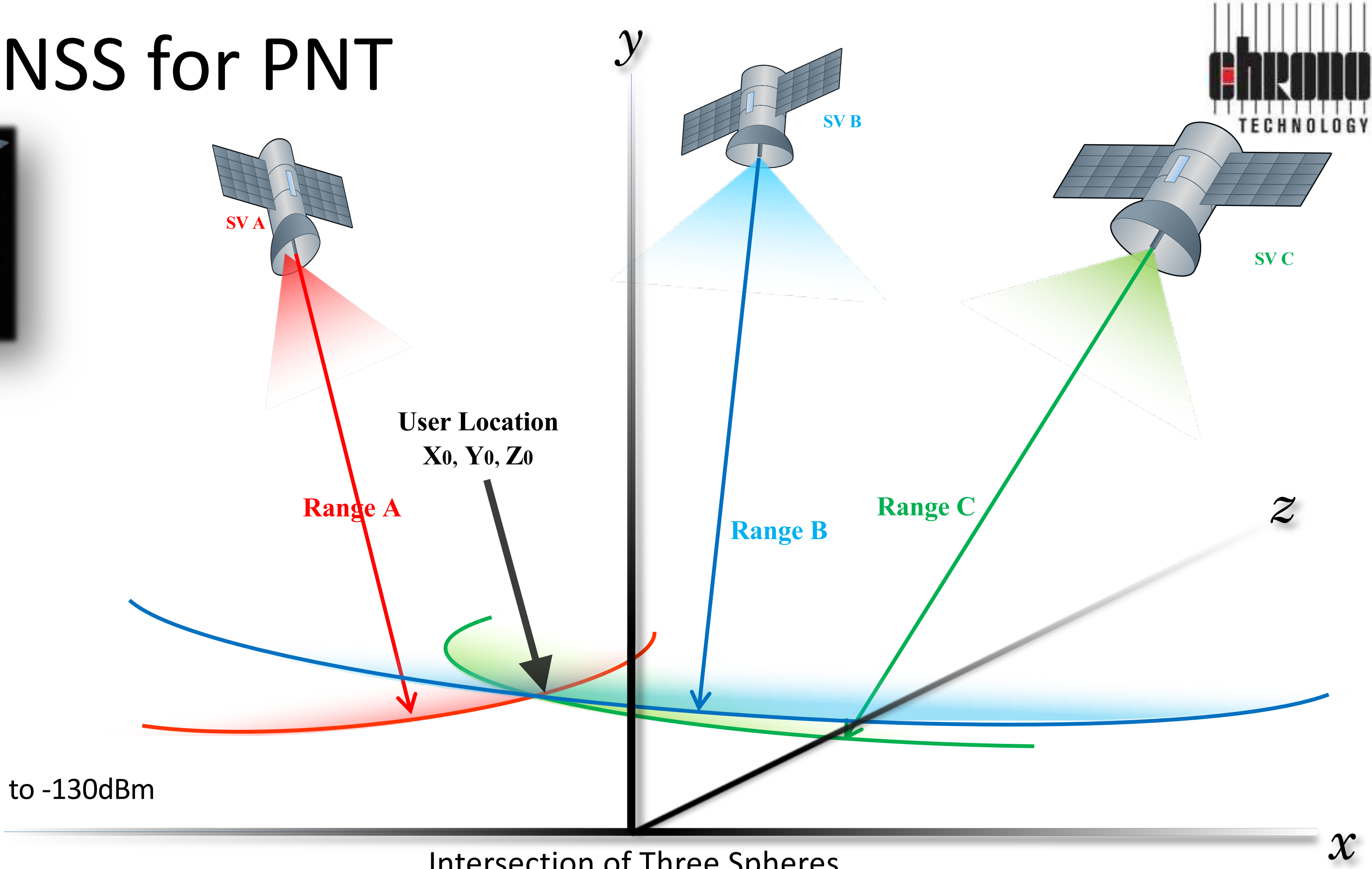
Using GNSS for PNT

MEO Satellites:
BEIDOU – 21,150 km
GALILEO – 23,222 km
GLONASS – 19,100 km
GPS – 20,200 km

Orbital period: 11-14hrs

Power output: 20-265W

Received signal: -125dBm to -130dBm



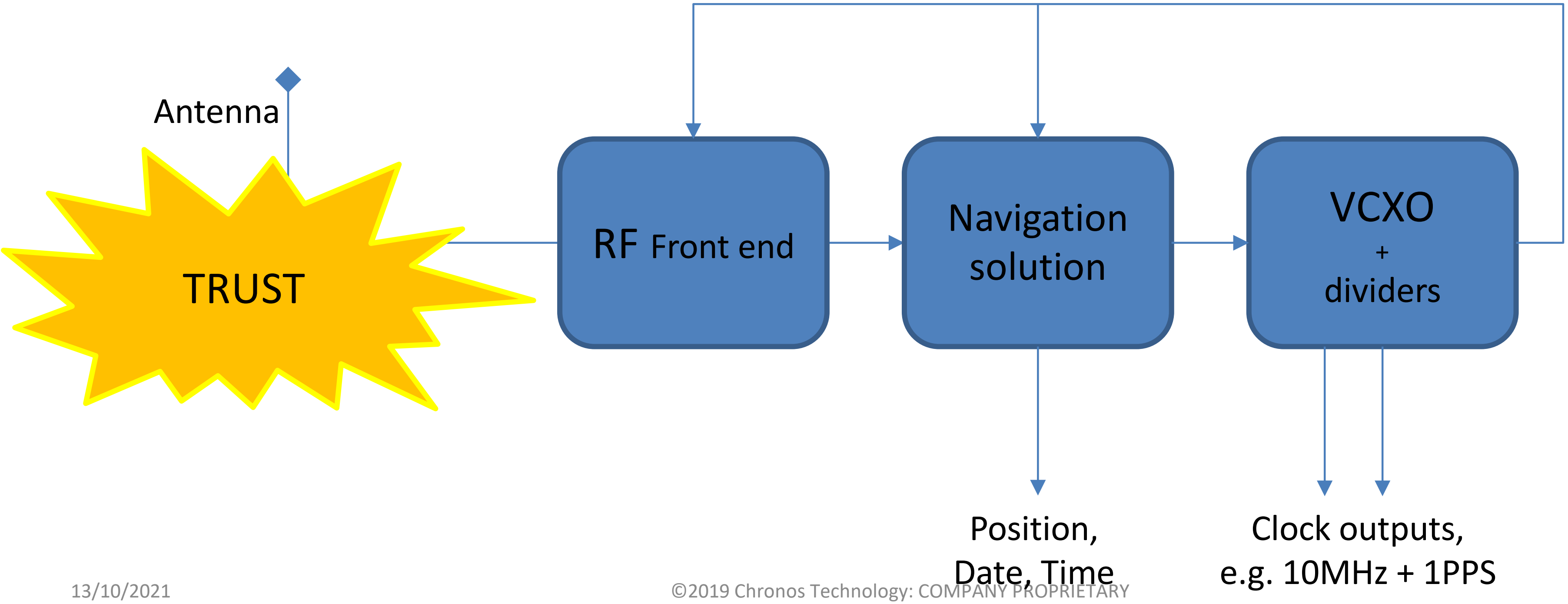
Intersection of Three Spheres

Receiver Clock (timing) errors add a 4th unknown, hence 4 satellites require for precise fix

13/10/2021

GNSS receiver – simplified view

- Uses the navigation solution to steer/control a local oscillator
- Timing output ultimately controlled by the RF signal input



The Problem

- "it's free and it works everywhere"
  - Proliferation of GPS receivers used for time
  - More than a billion GNSS receivers

- "it's free and it works everywhere all the time"
  - Phenomenal System uptime – a few major issues (e.g SVN23)
  - Fit-and-forget module/component/subsystem

- "GPS has us all addicted to Stratum 1 time"
  - NTP is everywhere – one of the oldest internet protocols
    - De-facto time sync service over packet networks

Jamming now a civilian activity

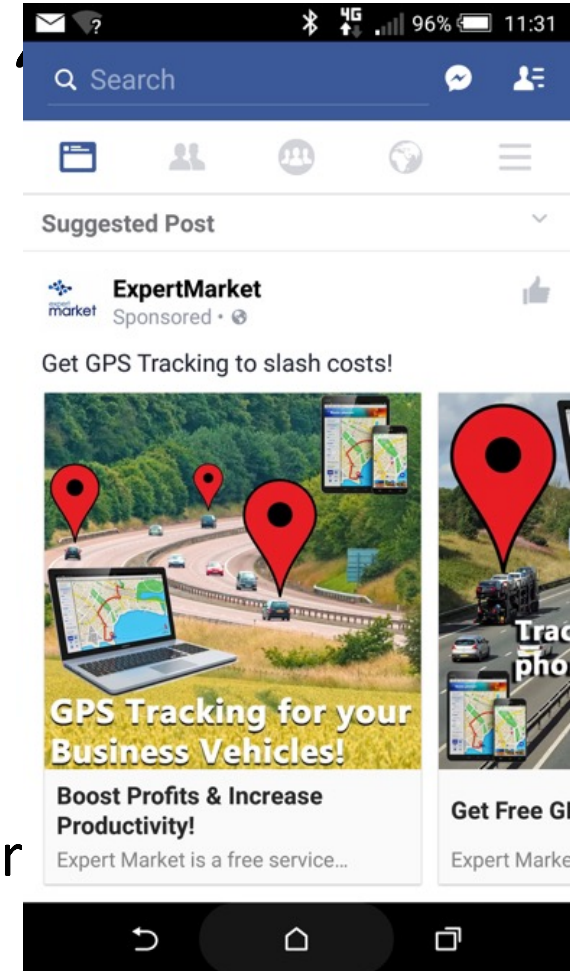
- Privacy concerns have lead to an explosion of “GPS Jammers”
  - Business/Fleet vehicle tracking
  - Offender tracking
  - Freight Tracking
  - High-value cars fitted with trackers
  - “Privacy Jammers” for sale on the internet
    - Some also jam GSM/3G/4G/WiFi/Bluetooth etc.
  - Personal privacy – criminal activity – organised crime

Jamming now a civilian activity

- Privacy concerns have lead to an explosion of "Jammers"
  - Business/Fleet vehicle tracking
  - Offender tracking
  - Freight Tracking
  - High-value cars fitted with trackers

  - "Privacy Jammers" for sale on the internet
    - Some also jam GSM/3G/4G/WiFi/Bluetooth etc.

  - Personal privacy – criminal activity – organised cr



Suggested Post

ExpertMarket
Sponsored ·

Get GPS Tracking to slash costs!

GPS Tracking for your Business Vehicles!

Boost Profits & Increase Productivity!

Expert Market is a free service...

Trac pho

Get Free Gl

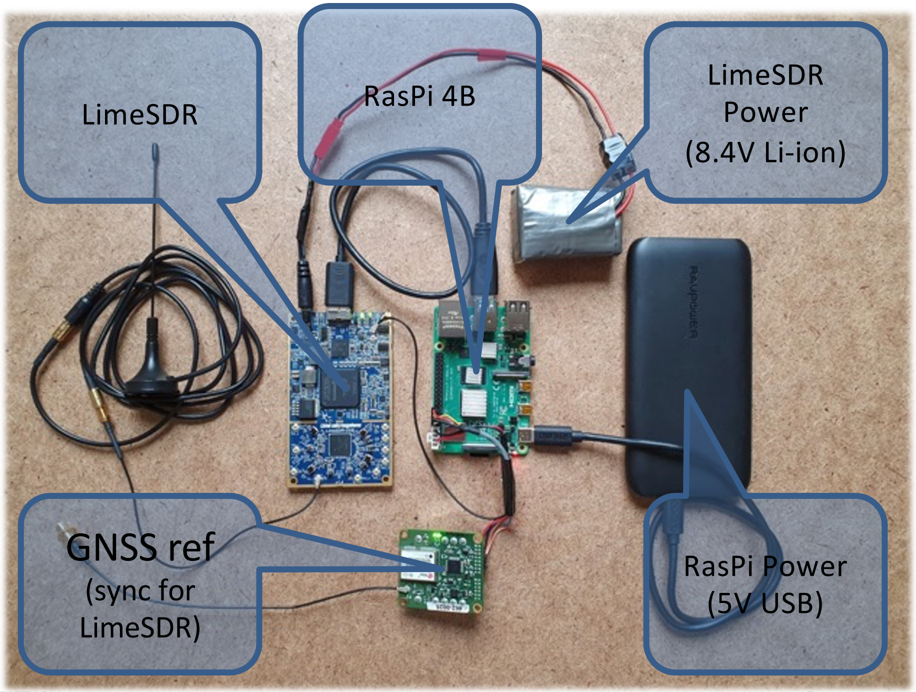
Expert Marke

Spoofing now a civilian activity

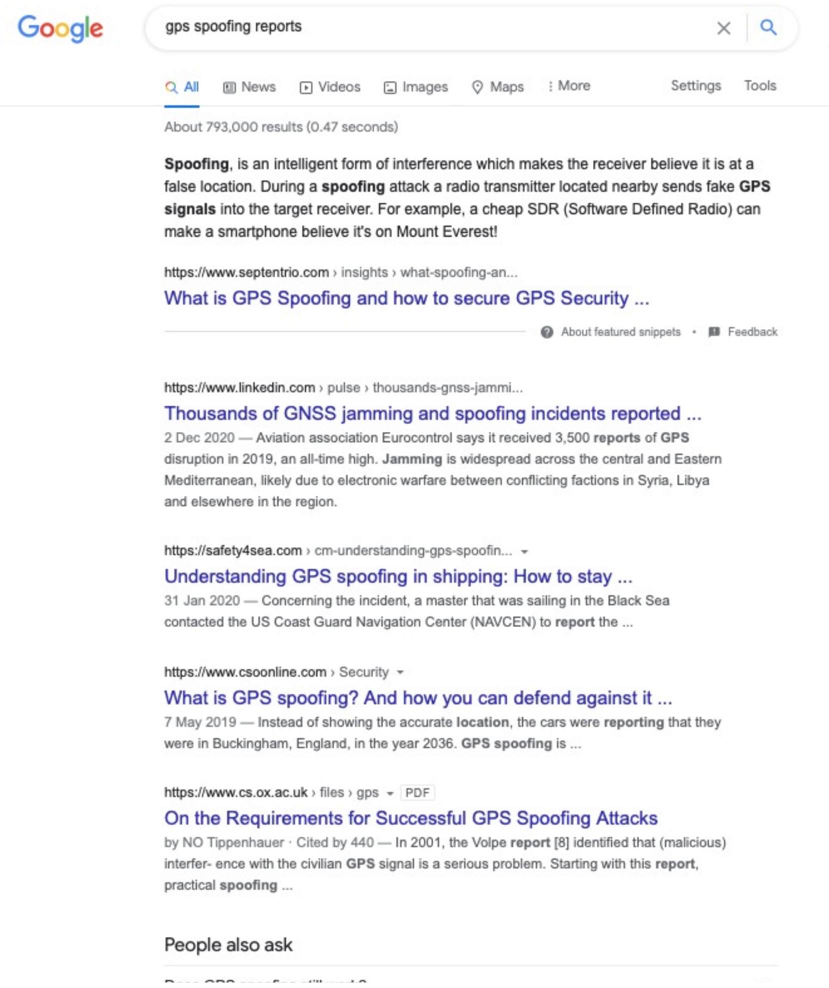
- Spoofing now trivial with COTS hardware & open-source software
  - Raspberry Pi + SDR + github code + electronics

- Increased use of location services has lead to widespread awareness of "Location Spoofing" techniques

- Of the receivers we tested
  - Some failed and needed power off/on reset
  - Some failed catastrophically needed to be re-flashed



But how common is it?



About 793,000 results (0.47 seconds)

Spoofing, is an intelligent form of interference which makes the receiver believe it is at a false location. During a **spoofing** attack a radio transmitter located nearby sends fake **GPS signals** into the target receiver. For example, a cheap SDR (Software Defined Radio) can make a smartphone believe it's on Mount Everest!

https://www.septentrio.com › insights › what-spoofing-an...
What is GPS Spoofing and how to secure GPS Security ...

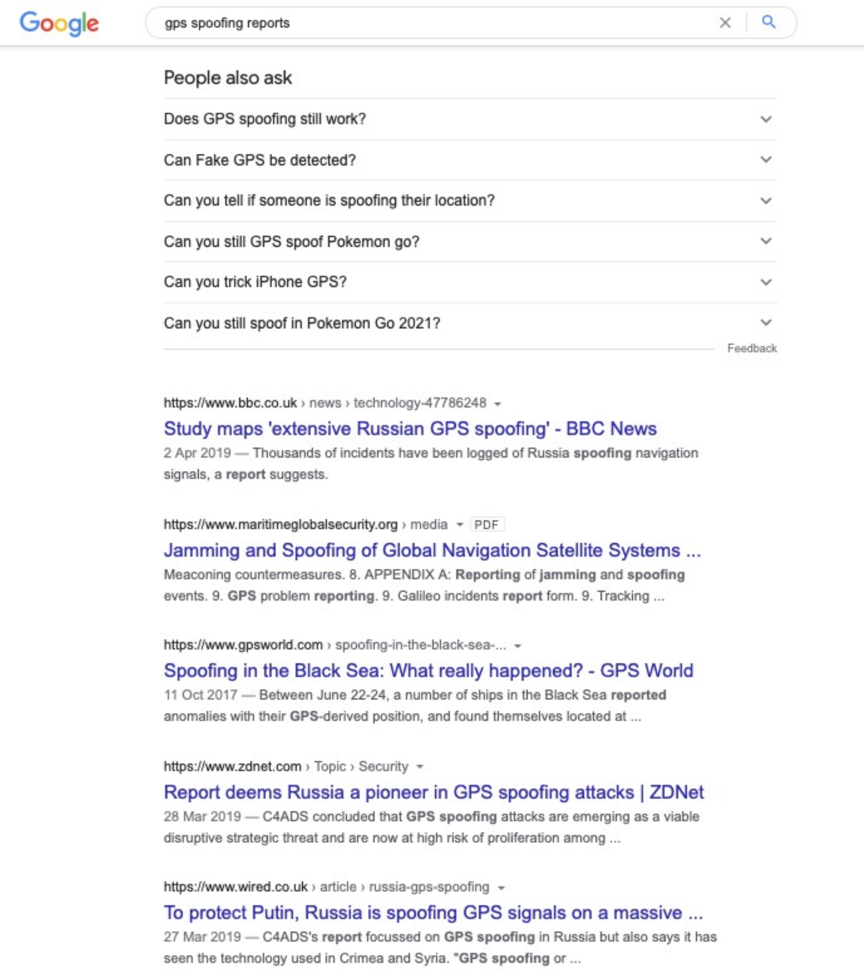
https://www.linkedin.com › pulse › thousands-gnss-jammi...
Thousands of GNSS jamming and spoofing incidents reported ...
2 Dec 2020 — Aviation association Eurocontrol says it received 3,500 **reports** of **GPS** disruption in 2019, an all-time high. **Jamming** is widespread across the central and Eastern Mediterranean, likely due to electronic warfare between conflicting factions in Syria, Libya and elsewhere in the region.

https://safety4sea.com › cm-understanding-gps-spoofin...
Understanding GPS spoofing in shipping: How to stay ...
31 Jan 2020 — Concerning the incident, a master that was sailing in the Black Sea contacted the US Coast Guard Navigation Center (NAVCEN) to **report** the ...

https://www.csoonline.com › Security
What is GPS spoofing? And how you can defend against it ...
7 May 2019 — Instead of showing the accurate **location**, the cars were **reporting** that they were in Buckingham, England, in the year 2036. **GPS spoofing** is ...

https://www.cs.ox.ac.uk › files › gps PDF
On the Requirements for Successful GPS Spoofing Attacks
by NO Tippenhauer · Cited by 440 — In 2001, the Volpe **report** [8] identified that (malicious) interfer- ence with the civilian **GPS** signal is a serious problem. Starting with this **report**, practical **spoofing** ...

People also ask



People also ask

- Does GPS spoofing still work?
- Can Fake GPS be detected?
- Can you tell if someone is spoofing their location?
- Can you still GPS spoof Pokemon go?
- Can you trick iPhone GPS?
- Can you still spoof in Pokemon Go 2021?

https://www.bbc.co.uk › news › technology-47786248
Study maps 'extensive Russian GPS spoofing' - BBC News
2 Apr 2019 — Thousands of incidents have been logged of Russia **spoofing** navigation signals, a **report** suggests.

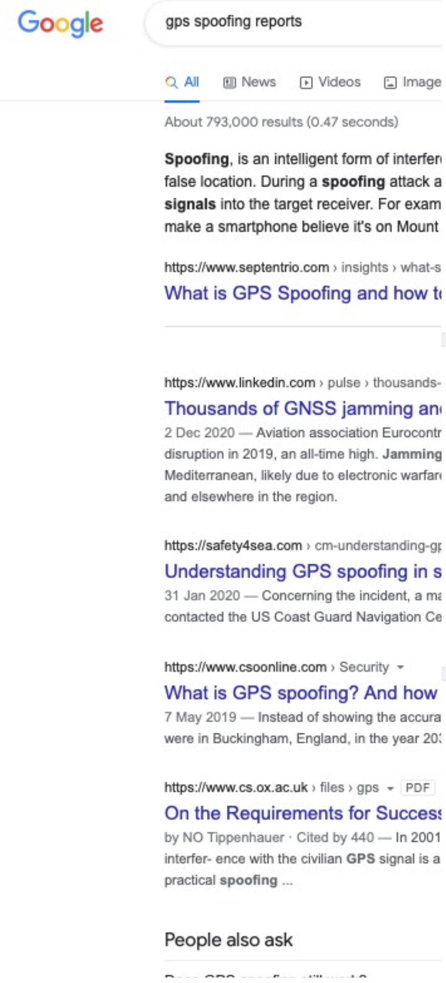
https://www.maritimeglobalsecurity.org › media PDF
Jamming and Spoofing of Global Navigation Satellite Systems ...
Meaconing countermeasures. 8. APPENDIX A: **Reporting** of **jamming** and **spoofing** events. 9. **GPS** problem **reporting**. 9. Galileo incidents **report** form. 9. Tracking ...

https://www.gpsworld.com › spoofing-in-the-black-sea-...
Spoofing in the Black Sea: What really happened? - GPS World
11 Oct 2017 — Between June 22-24, a number of ships in the Black Sea **reported** anomalies with their **GPS**-derived position, and found themselves located at ...

https://www.zdnet.com › Topic › Security
Report deems Russia a pioneer in GPS spoofing attacks | ZDNet
28 Mar 2019 — C4ADS concluded that **GPS spoofing** attacks are emerging as a viable disruptive strategic threat and are now at high risk of proliferation among ...

https://www.wired.co.uk › article › russia-gps-spoofing
To protect Putin, Russia is spoofing GPS signals on a massive ...
27 Mar 2019 — C4ADS's **report** focussed on **GPS spoofing** in Russia but also says it has seen the technology used in Crimea and Syria. "**GPS spoofing** or ...

But how common is it?



Google

gps spoofing reports

About 793,000 results (0.47 seconds)

Spoofing, is an intelligent form of interfer false location. During a **spoofing** attack a **signals** into the target receiver. For exam make a smartphone believe it's on Mount

https://www.septentrio.com › insights › what-s
What is GPS Spoofing and how t

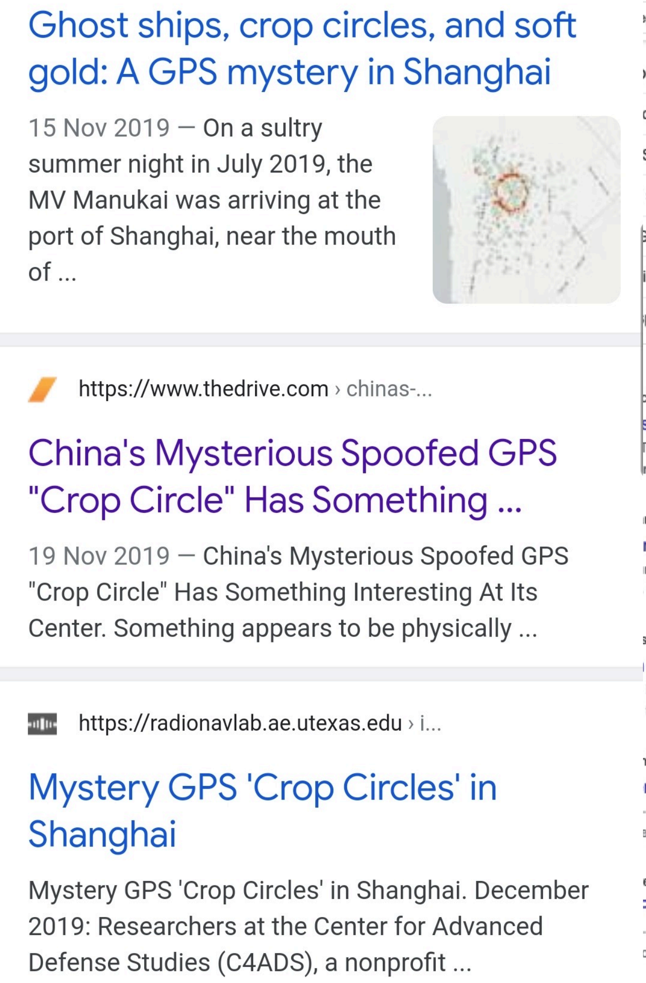
https://www.linkedin.com › pulse › thousands-
Thousands of GNSS jamming an
2 Dec 2020 — Aviation association Eurocontr disruption in 2019, an all-time high. **Jamming** Mediterranean, likely due to electronic warfar and elsewhere in the region.

https://safety4sea.com › cm-understanding-gp
Understanding GPS spoofing in s
31 Jan 2020 — Concerning the incident, a ma contacted the US Coast Guard Navigation Ce

https://www.csoonline.com › Security
What is GPS spoofing? And how
7 May 2019 — Instead of showing the accura were in Buckingham, England, in the year 20:

https://www.cs.ox.ac.uk › files › gps · PDF
On the Requirements for Success
by NO Tippenhauer · Cited by 440 — In 2001 interfer- ence with the civilian **GPS** signal is a practical **spoofing** ...

People also ask



Ghost ships, crop circles, and soft gold: A GPS mystery in Shanghai

15 Nov 2019 — On a sultry summer night in July 2019, the MV Manukai was arriving at the port of Shanghai, near the mouth of ...

https://www.thedrive.com › chinas-...

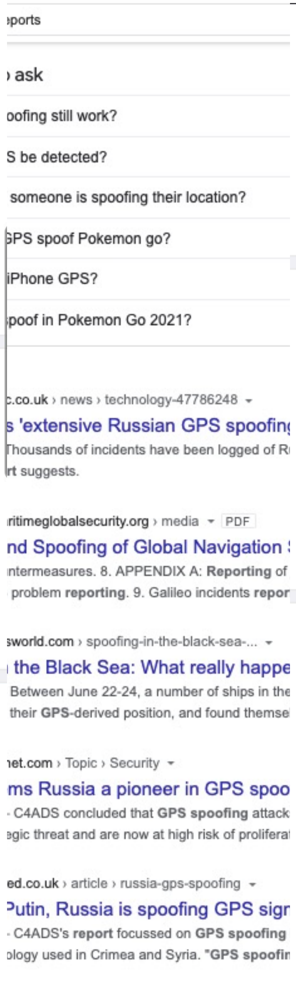
China's Mysterious Spoofed GPS "Crop Circle" Has Something ...

19 Nov 2019 — China's Mysterious Spoofed GPS "Crop Circle" Has Something Interesting At Its Center. Something appears to be physically ...

https://radionavlab.ae.utexas.edu › i...

Mystery GPS 'Crop Circles' in Shanghai

Mystery GPS 'Crop Circles' in Shanghai. December 2019: Researchers at the Center for Advanced Defense Studies (C4ADS), a nonprofit ...



ports

ask

oofing still work?

S be detected?

someone is spoofing their location?

GPS spoof Pokemon go?

iPhone GPS?

poof in Pokemon Go 2021?

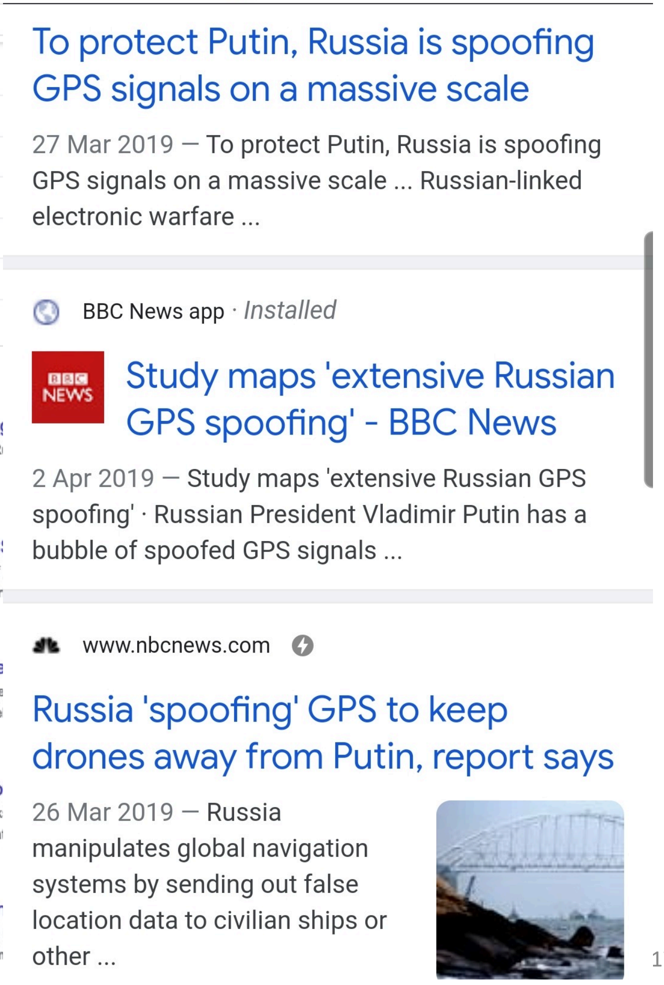
.co.uk › news › technology-47786248
s 'extensive Russian GPS spoofin
Thousands of incidents have been logged of R rt suggests.

ritimeglobalsecurity.org › media · PDF
nd Spoofing of Global Navigation
ntermeasures. 8. APPENDIX A: **Reporting** of problem **reporting**. 9. Galileo incidents **repor**

sworld.com › spoofing-in-the-black-sea-...
the Black Sea: What really happe
Between June 22-24, a number of ships in the their **GPS**-derived position, and found themse

net.com › Topic › Security
ms Russia a pioneer in GPS spoo
· C4ADS concluded that **GPS spoofing** attack egic threat and are now at high risk of prolifera

ed.co.uk › article › russia-gps-spoofing
Putin, Russia is spoofing GPS sign
· C4ADS's **report** focussed on **GPS spoofing** ology used in Crimea and Syria. "**GPS spoofin**



To protect Putin, Russia is spoofing GPS signals on a massive scale

27 Mar 2019 — To protect Putin, Russia is spoofing GPS signals on a massive scale ... Russian-linked electronic warfare ...

BBC News app · *Installed*

Study maps 'extensive Russian GPS spoofing' - BBC News

2 Apr 2019 — Study maps 'extensive Russian GPS spoofing' · Russian President Vladimir Putin has a bubble of spoofed GPS signals ...

www.nbcnews.com

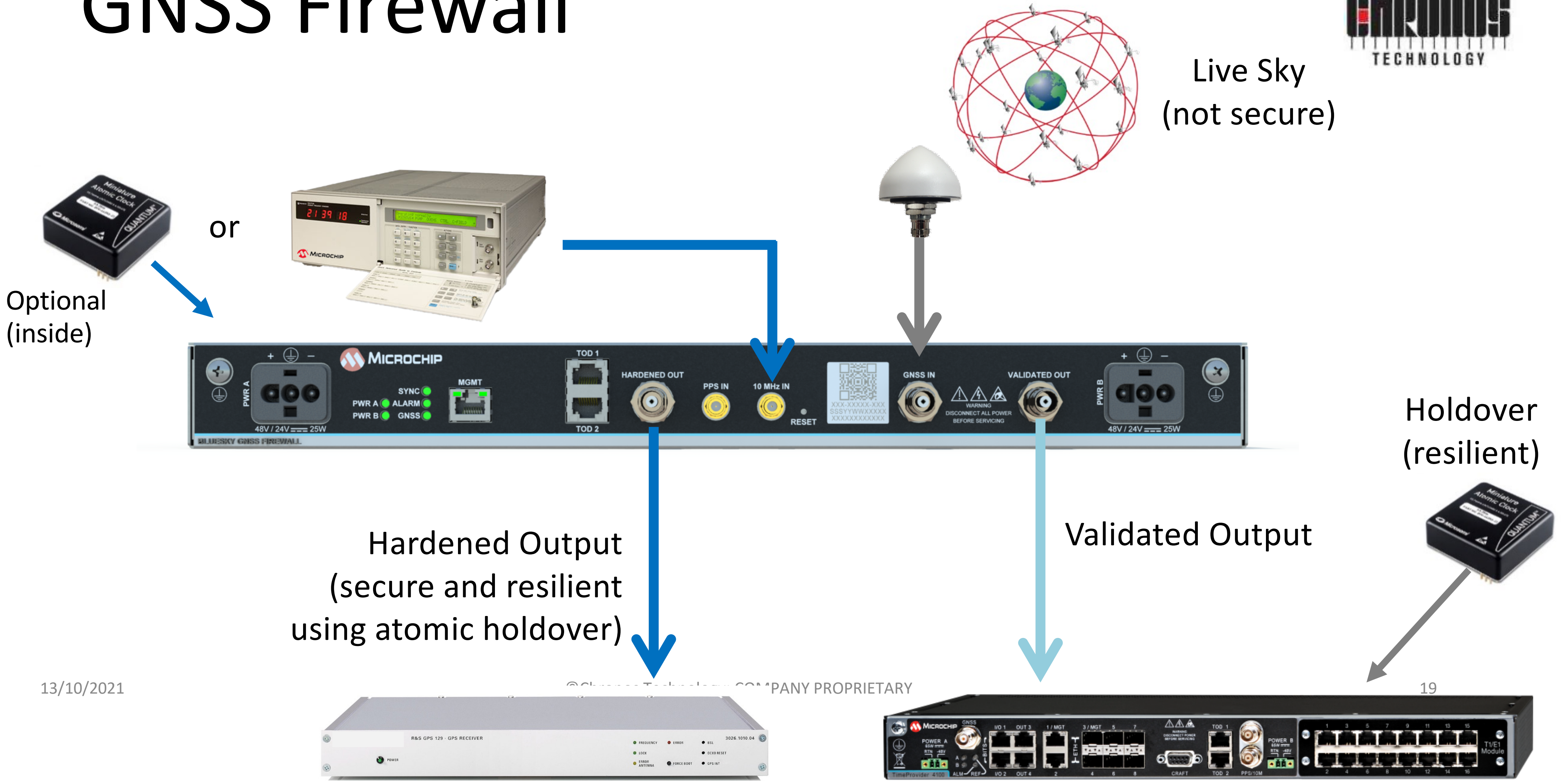
Russia 'spoofing' GPS to keep drones away from Putin, report says

26 Mar 2019 — Russia manipulates global navigation systems by sending out false location data to civilian ships or other ...

GNSS Firewall

- Provides a much deeper level of signal analysis
  - Simple spoofers have many data fields left at defaults
  - Detects anomalies in power, time, position, data
- Contains a GPS signal simulator, accurately sync'd to GNSS to maintain PNT for any downstream devices

GNSS Firewall



Live Sky
(not secure)

or

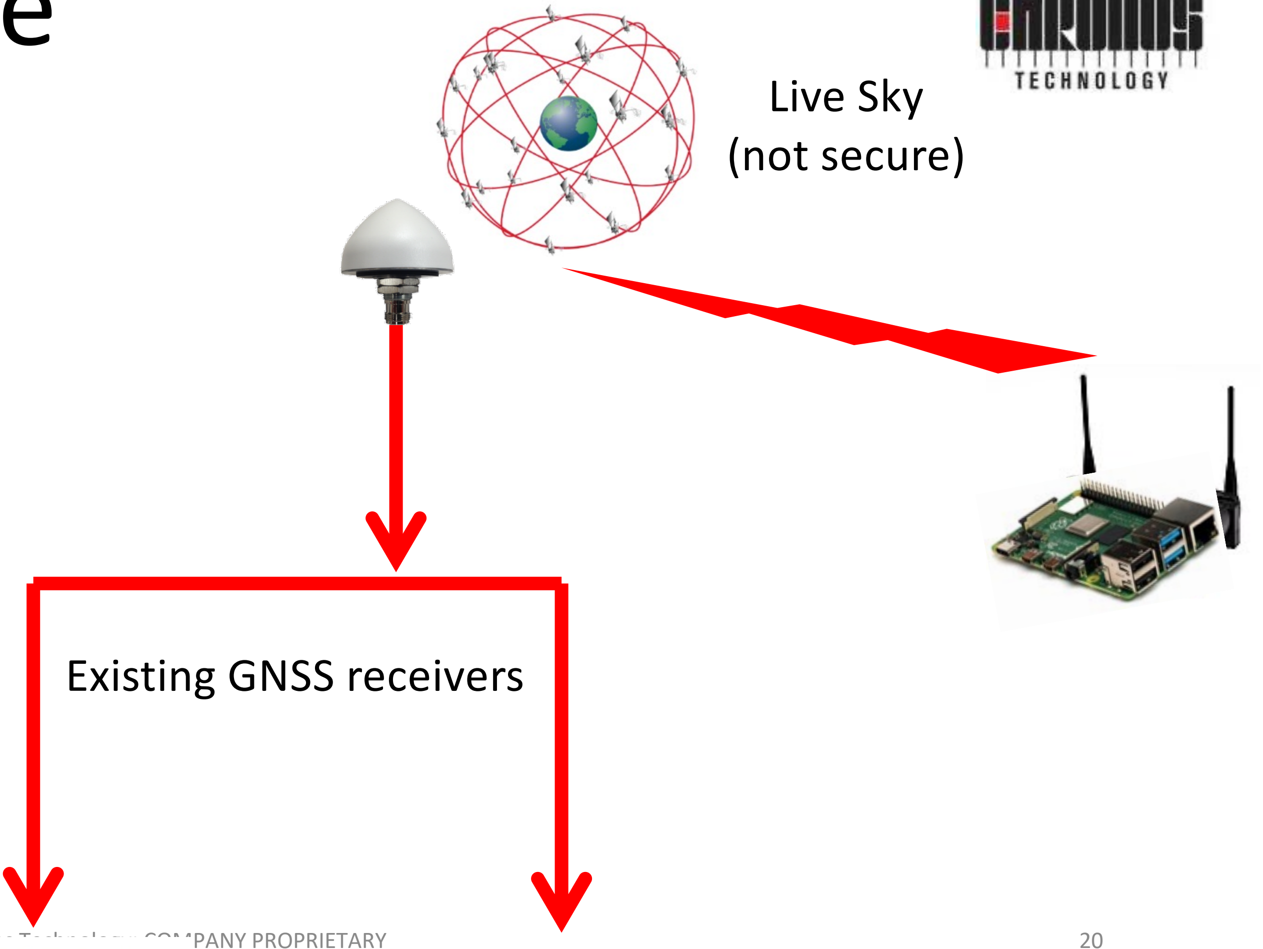
Optional
(inside)

Holdover
(resilient)

Hardened Output
(secure and resilient
using atomic holdover)

Validated Output

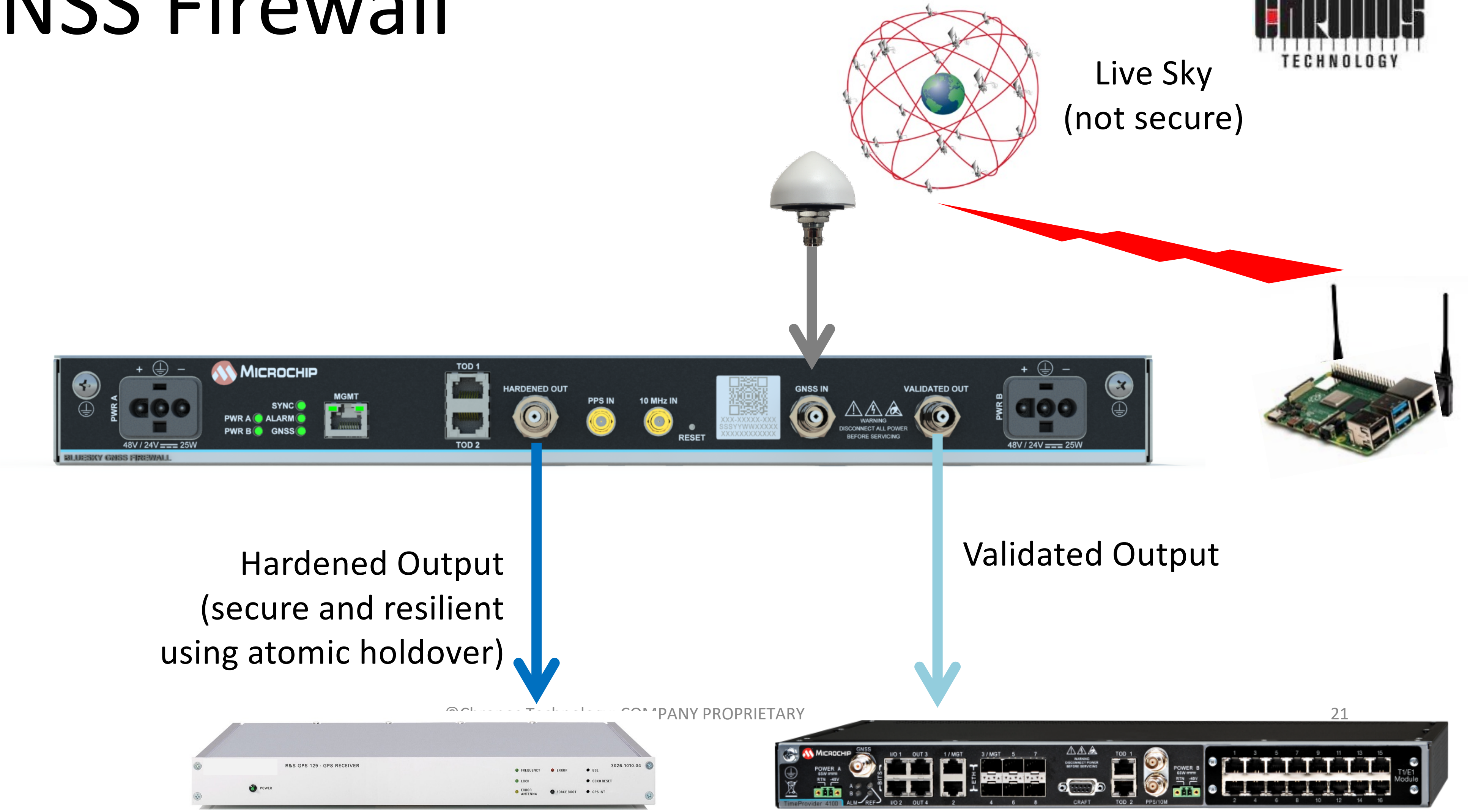
GNSS vulnerable



Live Sky
(not secure)

Existing GNSS receivers

GNSS Firewall

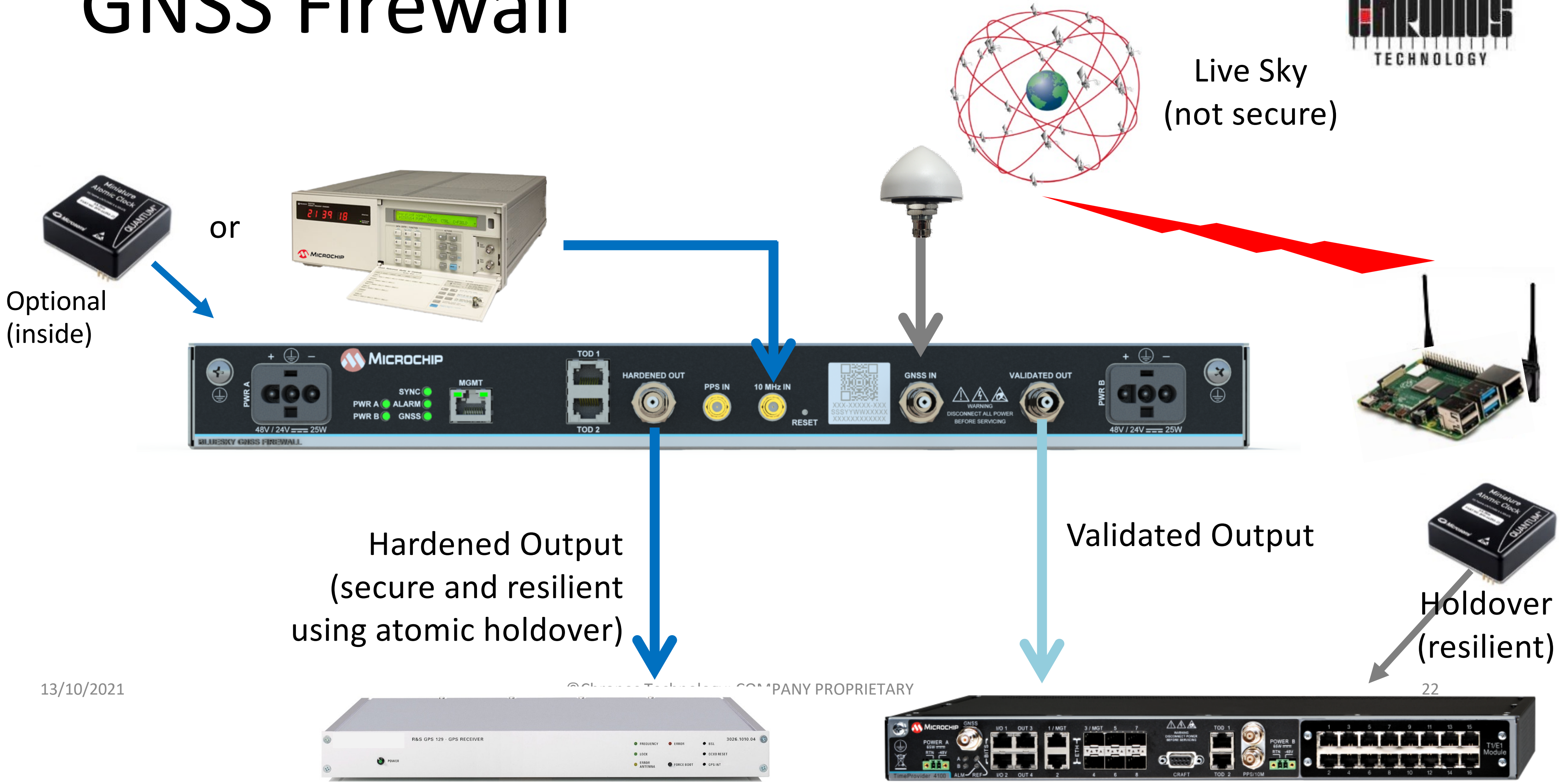


Live Sky
(not secure)

Hardened Output
(secure and resilient
using atomic holdover)

Validated Output

GNSS Firewall



Live Sky
(not secure)

Optional
(inside)

or

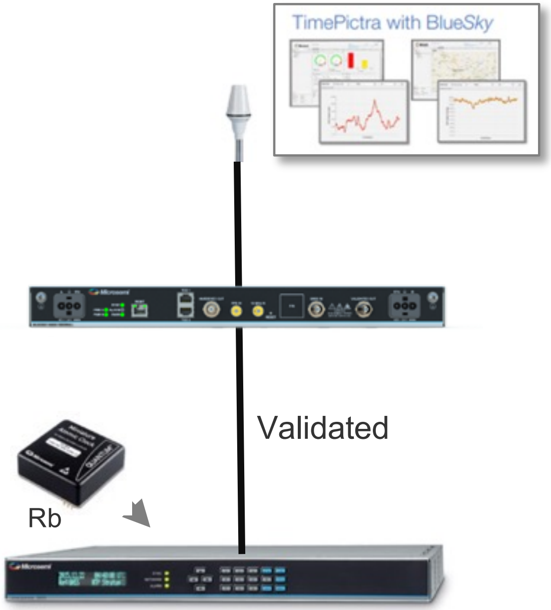
Hardened Output
(secure and resilient
using atomic holdover)

Validated Output

Holdover
(resilient)

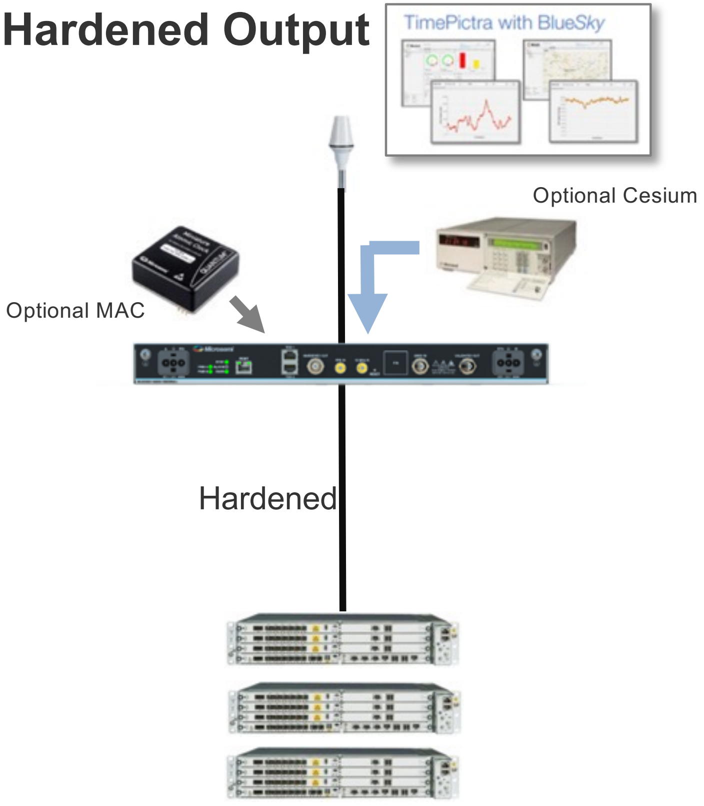
GNSS Firewall Deployment models

Firewall using Validated Output



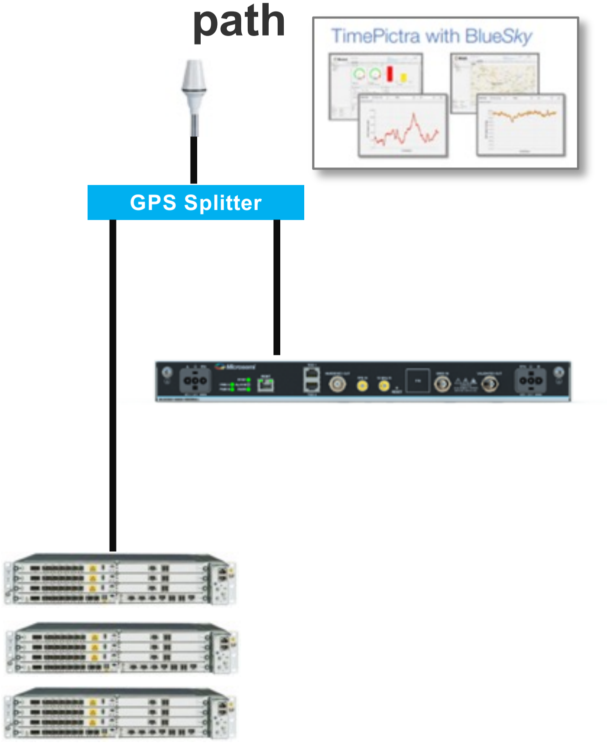
NTP/PTP SyncServer etc.

Firewall using Hardened Output



Equipment requiring GPS/L1 signal

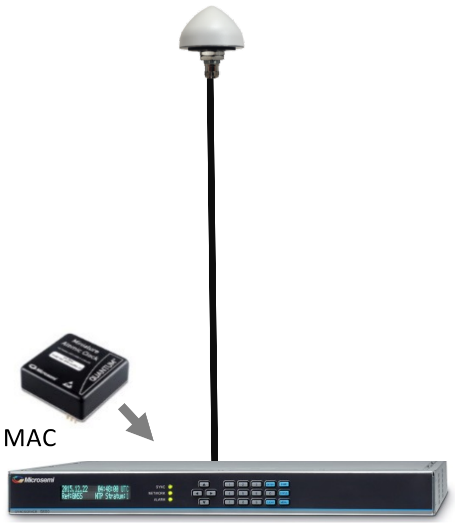
Firewall deployed for monitoring, not in GPS signal path



Equipment requiring GPS/L1 signal

Resilient Timing Deployment models

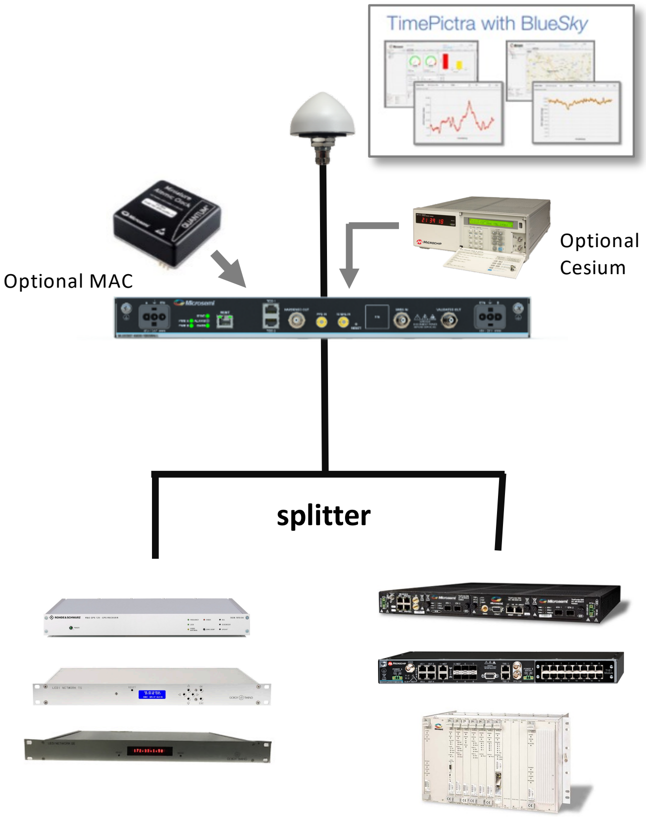
Time Server with GNSS firewall features inside



MAC

SyncServer

Firewall for timing protection of "legacy" products



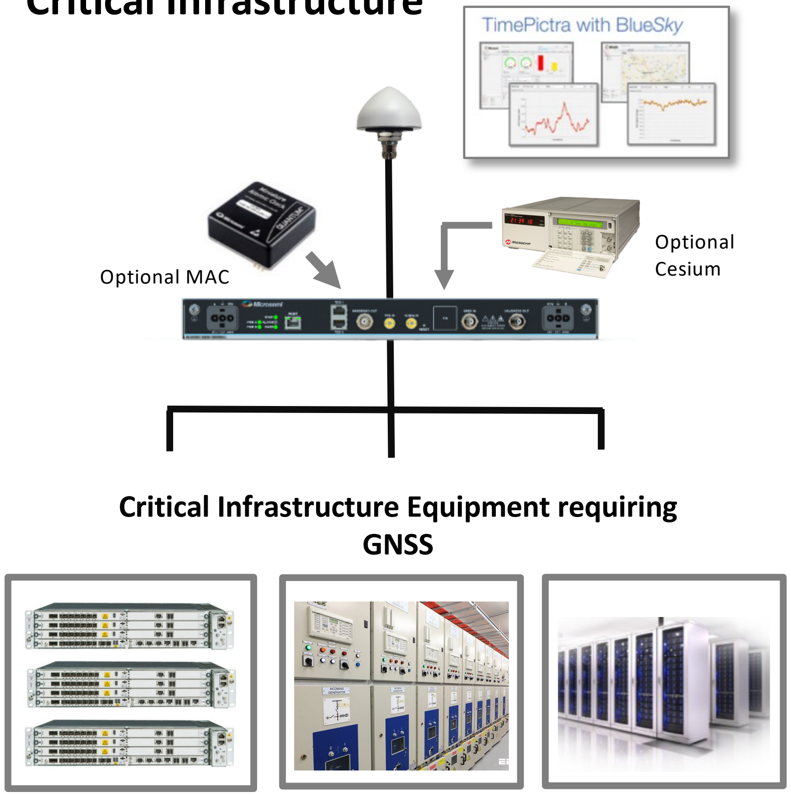
TimePictra with BlueSky

Optional MAC

Optional Cesium

splitter

Firewall for PNT protection of Critical Infrastructure



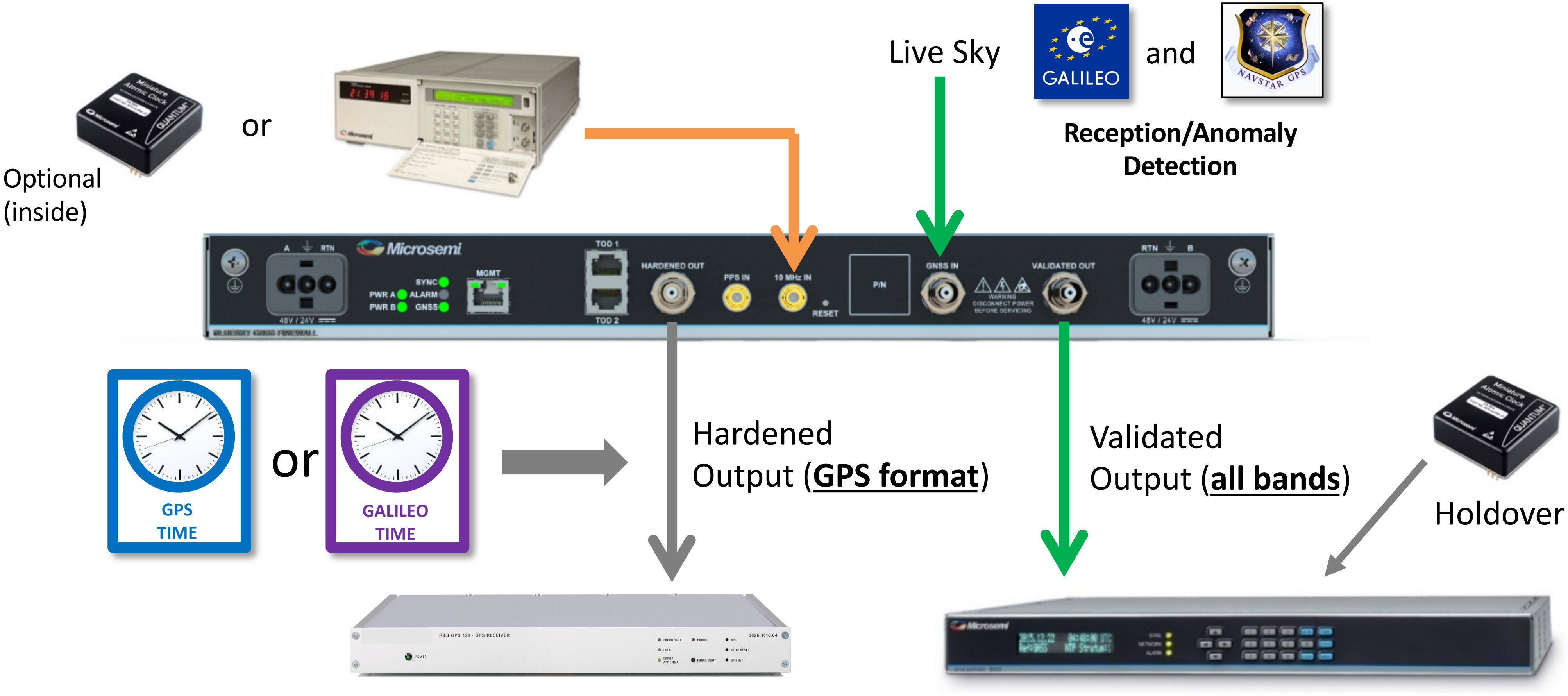
TimePictra with BlueSky

Optional MAC

Optional Cesium

Critical Infrastructure Equipment requiring GNSS

Support for Galileo



Optional (inside)

or

Live Sky

and

Reception/Anomaly Detection

GPS TIME

or

GALILEO TIME

Hardened Output (**<u>GPS format</u>**)

Validated Output (**<u>all bands</u>**)

Holdover

Positioning - Underground

- Many solutions to positioning inside
  - Proprietary solutions/signals/”Sensor fusion” wi-fi/Bluetooth/Optical(camera)/gyro
  - Need dedicated receiver h/w & s/w
- But, what about using GPS-like signals?
  - Compatibility with millions of hand-held devices (Smartphones, NAV receivers, TETRA radios etc.)

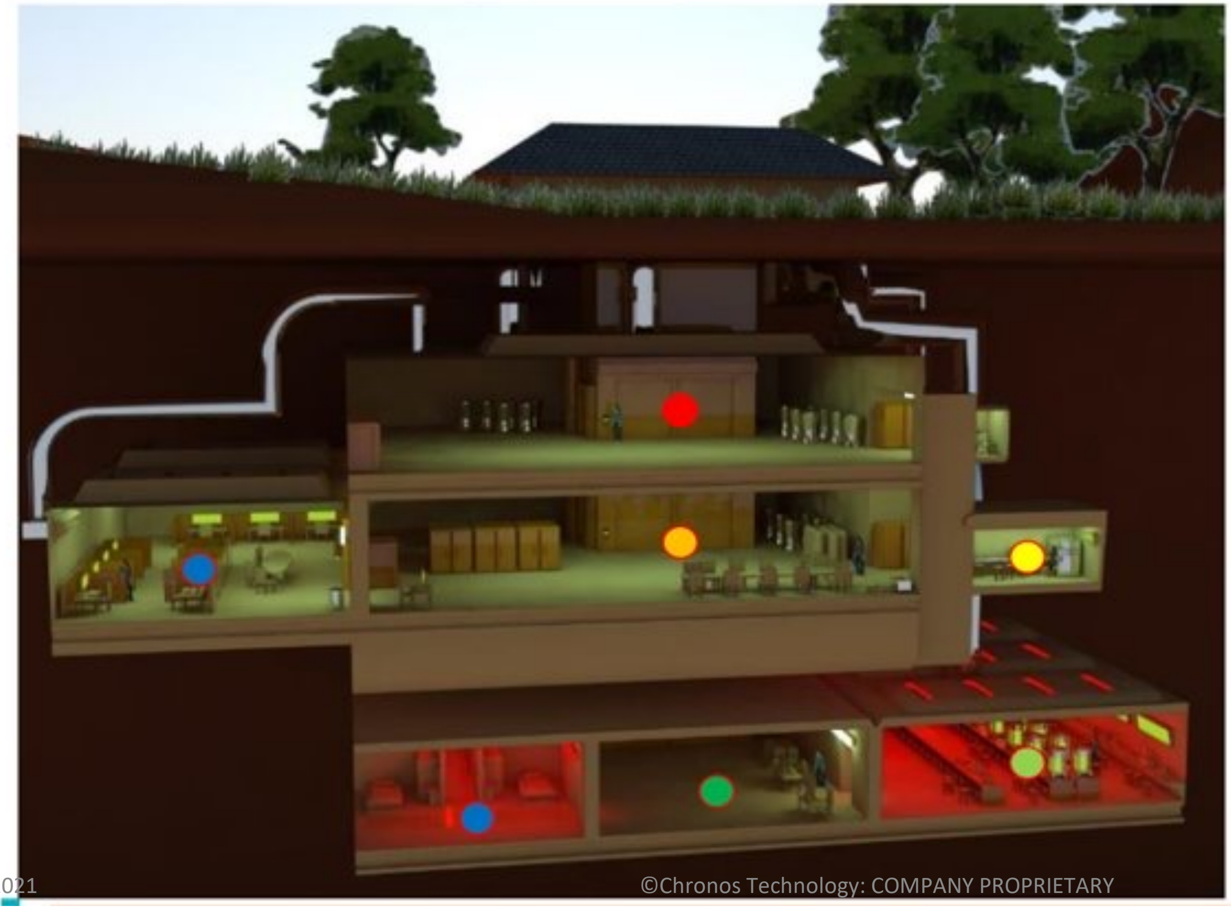
Using a ”spoofer” for positioning?

- Tunnels – transport (road/rail)
- Existing infrastructure may already be there – “leaky feeders” used to re-broadcast FM/DAB/4G radio
- Broadcast a simulated signal that you would see at that location if the sky were visible (i.e. altitude adjusted)
- Time/Date sync’d to real GNSS from the sky

- Broadcast an additional unused PRN-code (not contained in real GPS almanac so ignored by receivers) as a test signal to make sure simulated signal can’t be seen outside of the underground space

Zone based

DEPLOYMENT INSIDE BUILDINGS



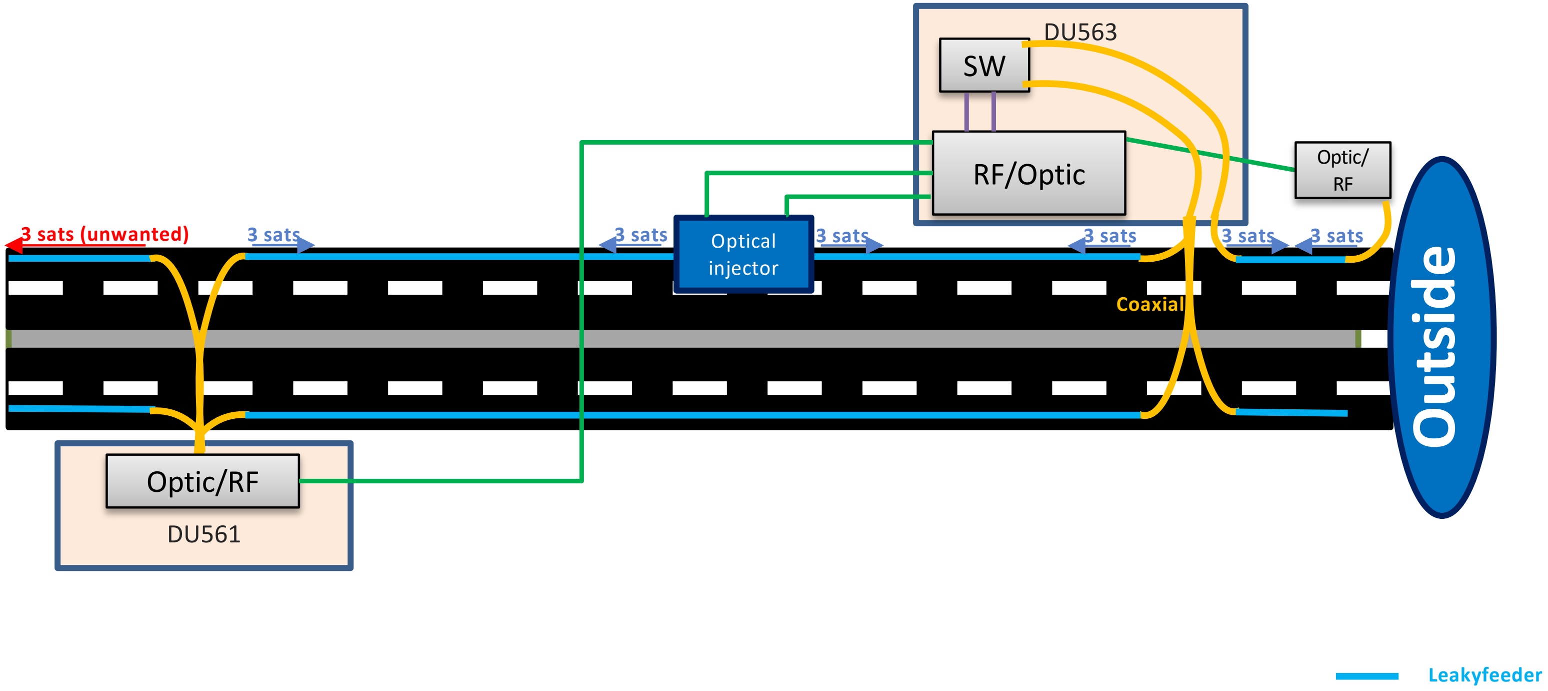
- Simulated static position is the centre of each zone

Example of installation of SW in building basement:

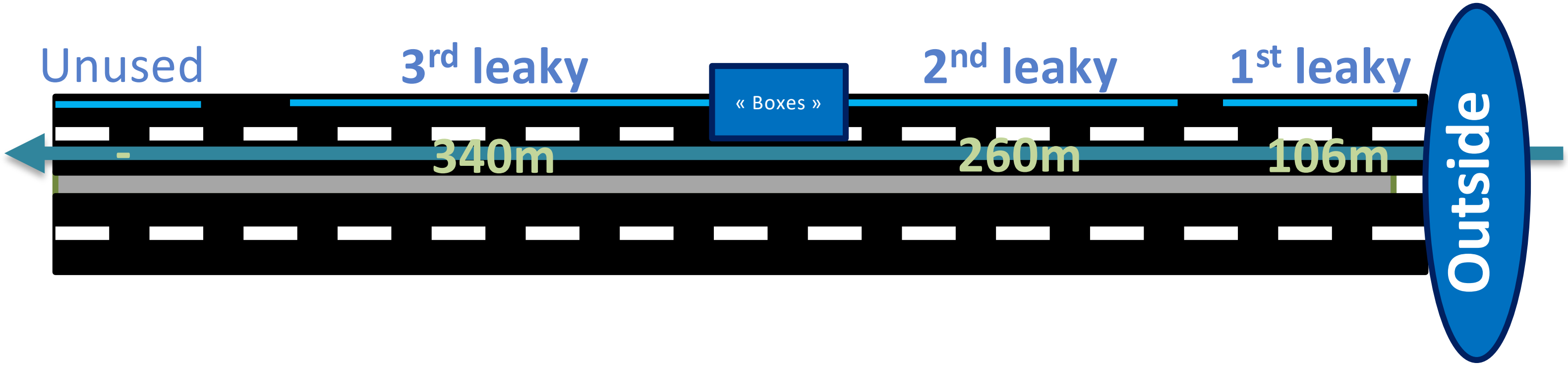
✓ Zone 1 🔴 SW
✓ Zone 2 🟠 SW
✓ Zone 3 🟡 SW
✓ Zone 4 🟢 SW
✓ Zone 5 🟢 SW
✓ Zone 6 🔵 SW
✓ Zone 7 🔵 SW

In Zones 1 to 7, the GPS value given by your receiver corresponds to the room center

GNSS Continuous - Road Tunnels

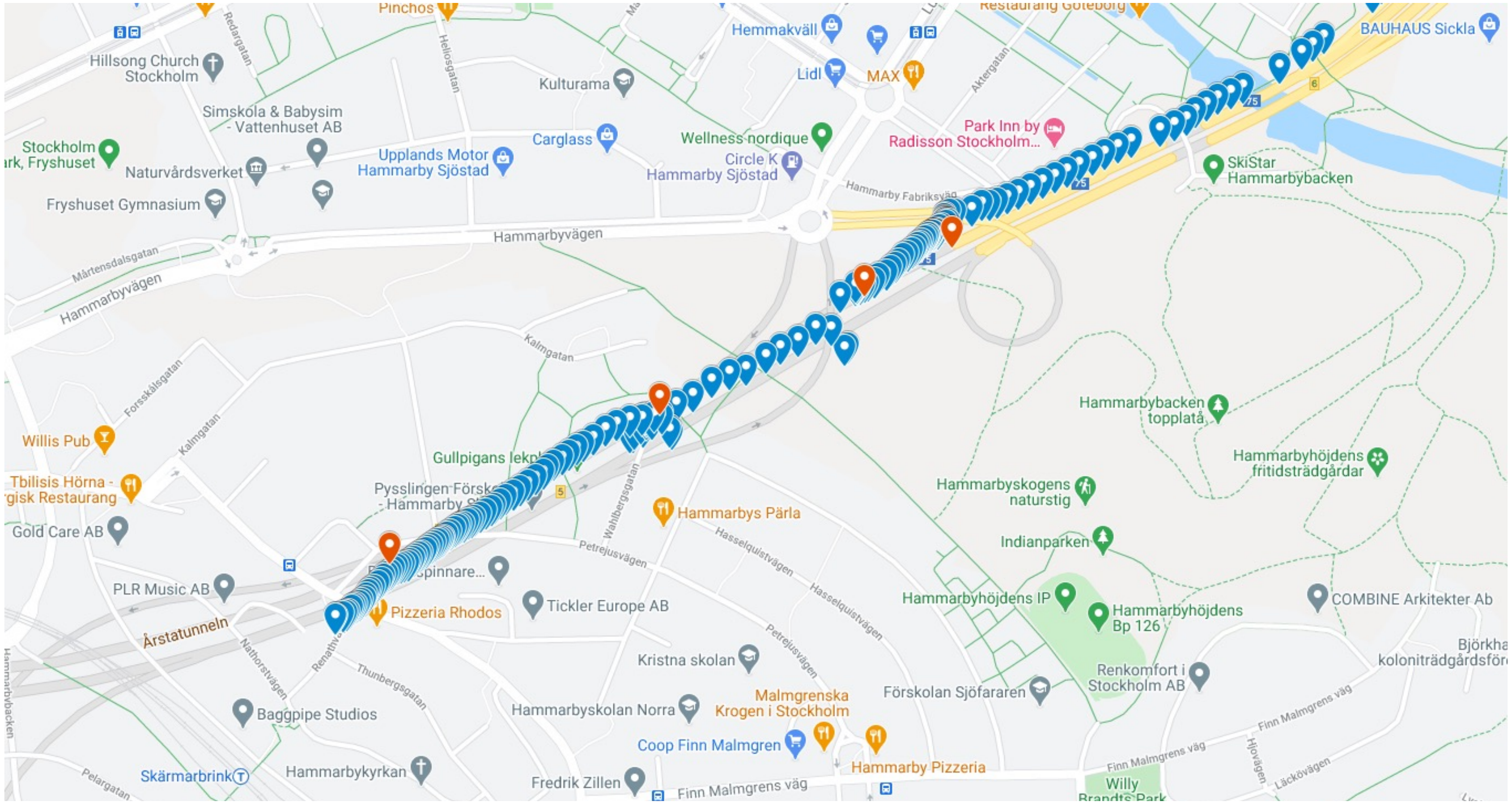


GNSS Continuous - Road Tunnels



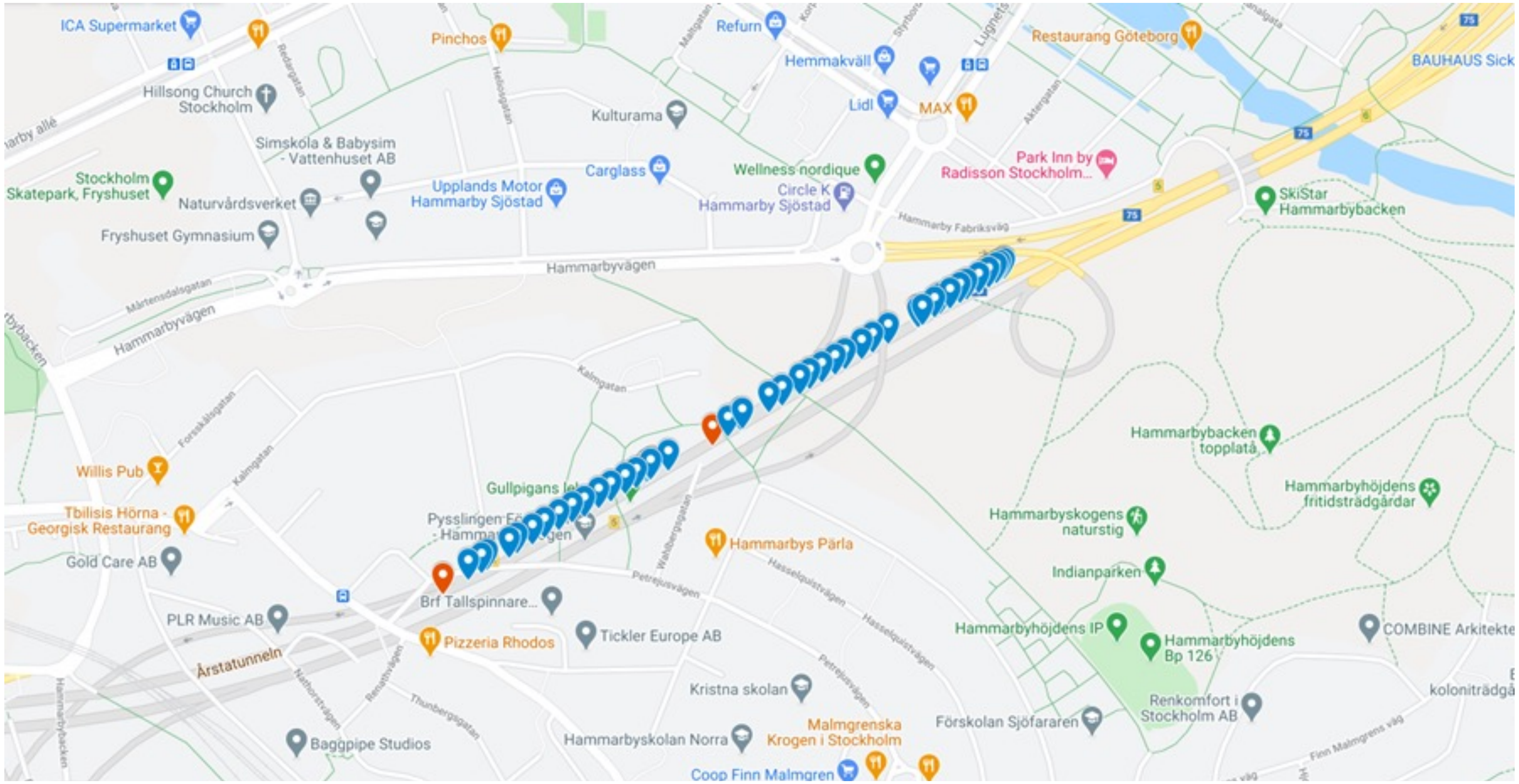
GNSS Continuous - Road Tunnels

- High-speed test - 60-70km/h drive



GNSS Continuous - Road Tunnels

- Android smartphone ~70km/h drive



Conclusions

- Simulation of GNSS signals has become (almost) trivial

- But - “controlled spoofing” can provide
  - Protection to Critical Infrastructure that relies on GNSS
  - New opportunities to increase the safety of emergency workers/civilians and enable continuous asset-tracking in GNSS-denied areas

ITSF 2021 – Brighton, UK

Christian Farrow B.Sc. (Hons) MinstP MIET
Technical Services Manager

@ChronosTechno

Turning the Tables on the Spoofers

- “self-spoofing” systems supplying secure signals to augment existing PNT receivers.

CHRONOS TECHNOLOGY