FORSBERG

POSITIONING | NAVIGATION | TIMING

Hydrographic Society
GNSS Interferentie en Spoofing

Jammer Detection

Charles Forsberg

New Branding and New Office

FORSBERG
POSITIONING | NAVIGATION | TIMING

Relative Powers
GNSS and Interference

FORSBERG
POSITIONING | NAVIGATION | TIMING

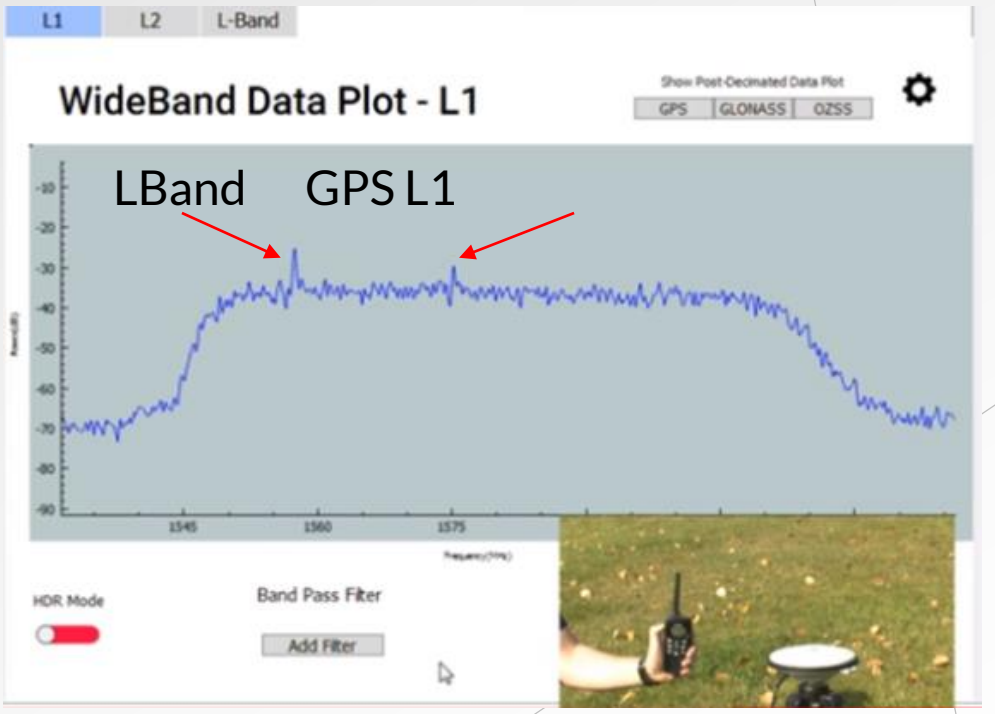
The Power of the GPS Signal

- **Signal Strengths at the earth's surface**
- L1 has a typical signal strength of -130.0dBm (~1.0 x 10e-16 W)*
- L2 has a typical signal strength of -127.5dBm (~1.8 x 10e-16 W)*
- L5 has a typical signal strength of -127.6dBm (~1.74 x 10e-16 W)*

** Prior to any antenna gain*

- The satellite's transmitted signal strength is:
  - Transmitter = ~25W
  - Antenna = ~13dBi
  - **Totalling ~500W (~ +57dBm)**

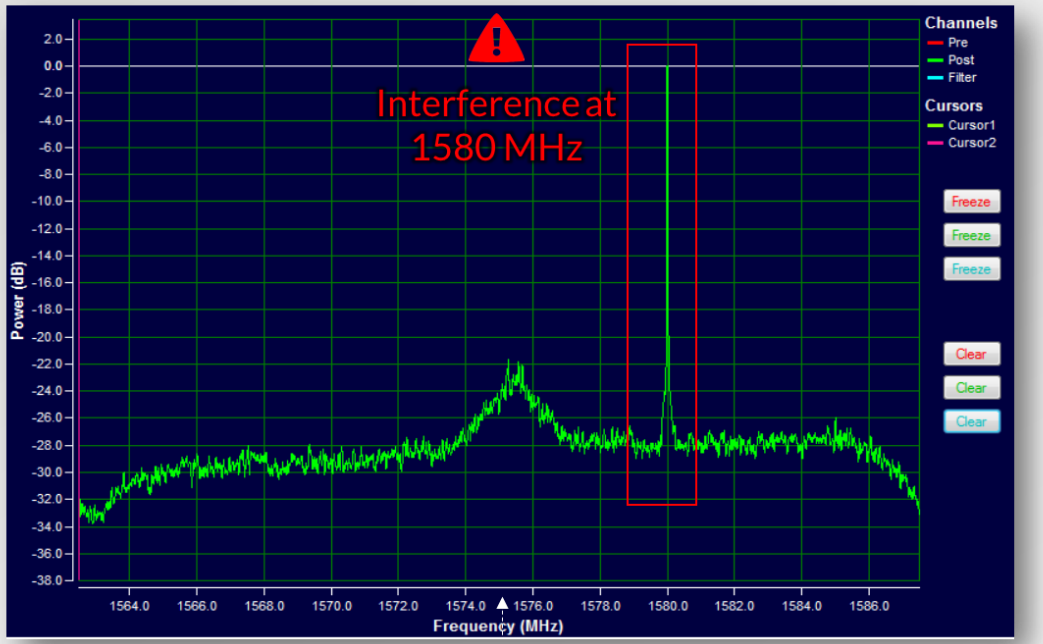
- The balance of ~ 184dBm get's lost in transit from satellite to the majority of users.
- **A GPS signal at the earth's surface is approximately 2*10e-16 Watts (tiny)**

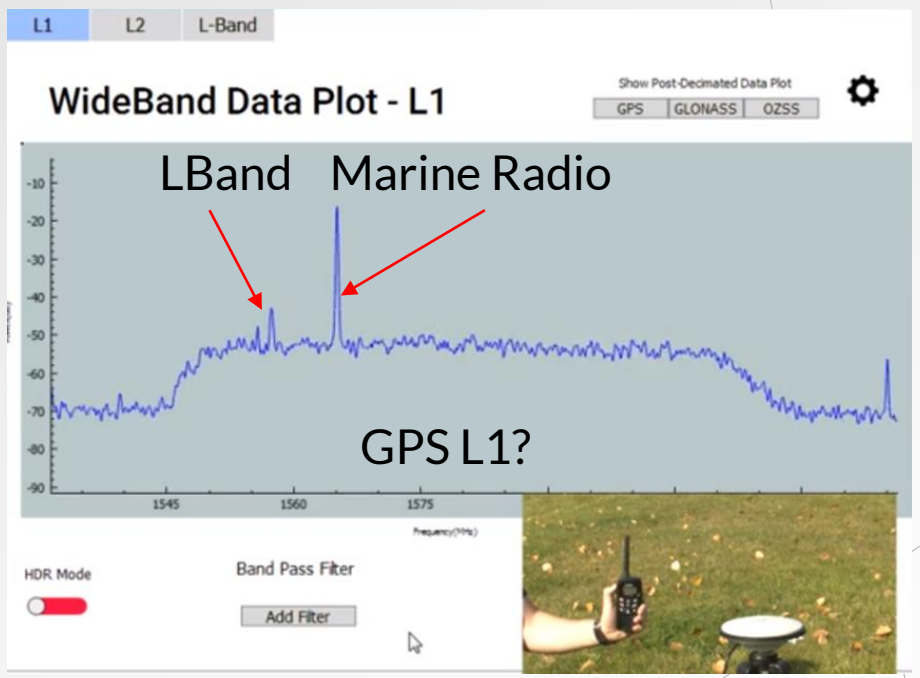


FORSBERG
POSITIONING | NAVIGATION | TIMING

The Power of the Interference Signal

- An interference source is relatively powerful and can be achieved at very low power levels measured in fractions of a Milliwatt. This example is extremely low power but can jam GPS
- From the previous slide we know that the GPS signal at the earth's surface is ~ 2*10e-16 Watts
- **Interference Power is ~ 2.0*e-14 Watts (~100 times more powerful than GPS)**





FORSBERG
POSITIONING | NAVIGATION | TIMING

Transmit and Receive Jammers and GNSS Antennas

FORSBERG
POSITIONING | NAVIGATION | TIMING

Typical Sources of GNSS Denial

- **Jamming** - Accidental to intentional
- **Meaconing** – Typically accidental – faulty equipment
- **Spoofing** – Generally 100% intentional

Good
Military Training

Bad
Commercially Available

Ugly
Organised Crime and Hostile Military

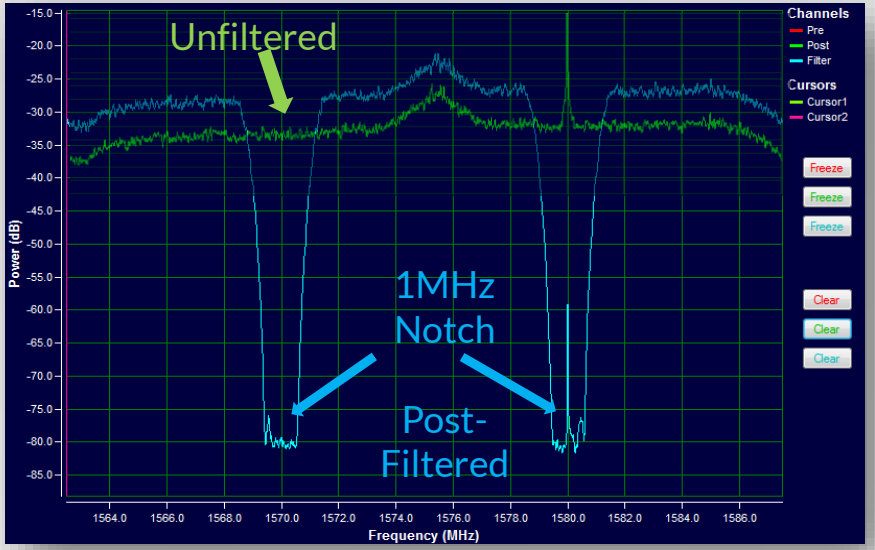
FORSBERG
POSITIONING | NAVIGATION | TIMING

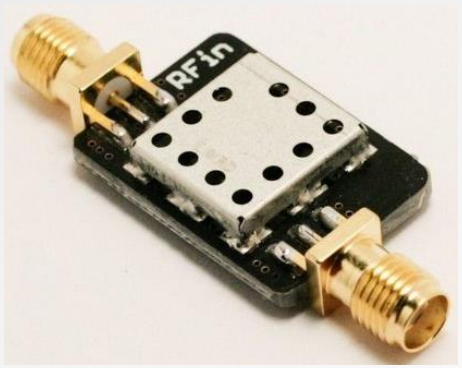
Mitigation Methods

- Improved antenna – e.g. Survey Grade vs Helical
- Software filters as offered on some receivers
- Hardware filters
- Anti-Jam antenna such as NovAtel GAJT
- A combination of these will produce enhancements

Survey Grade Antenna

Helical Antenna



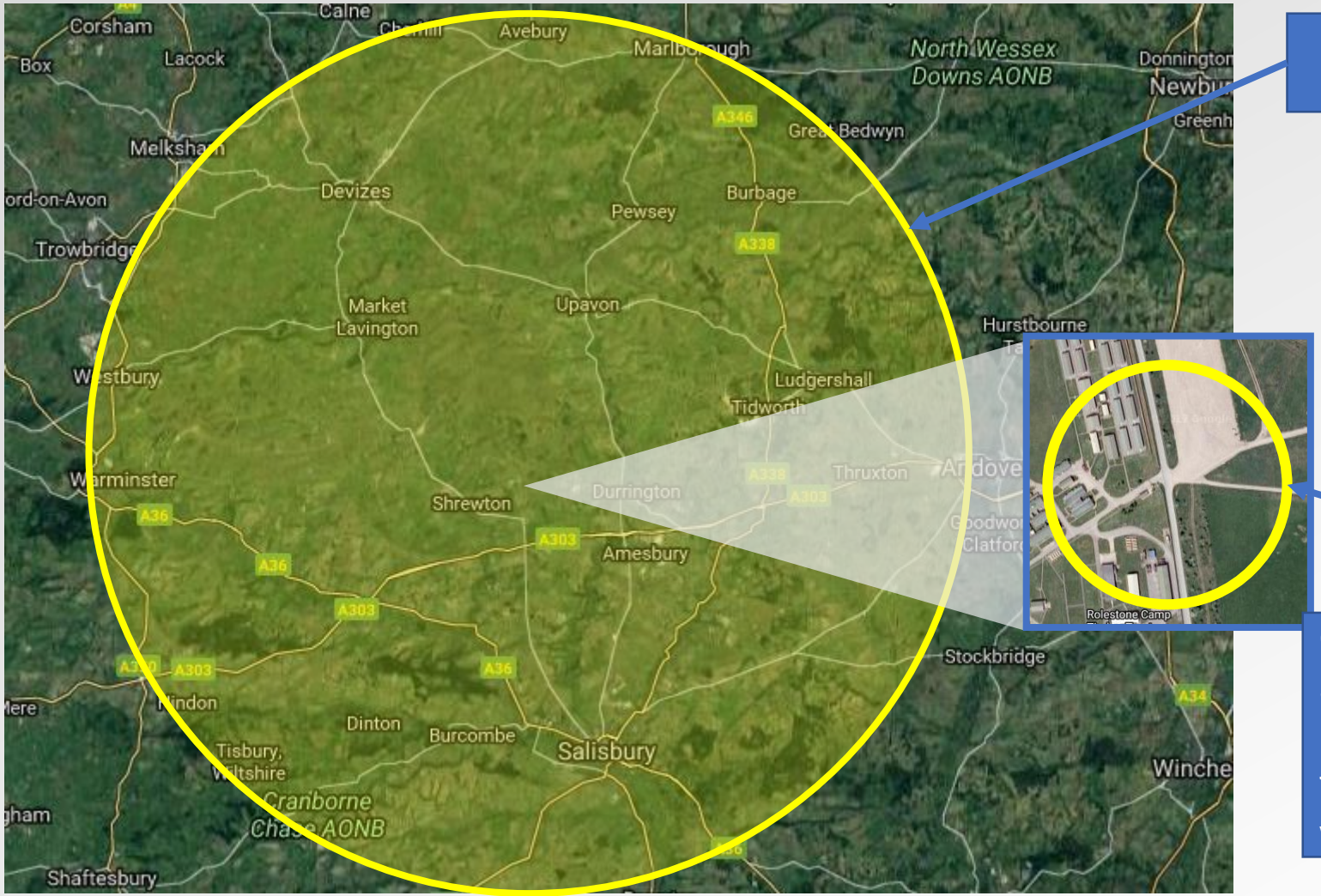


Hardware Filters

Anti-Jam Antenna

FORSBERG
POSITIONING | NAVIGATION | TIMING

GAJT REDUCES THE EFFECT OF JAMMING BY >99%



A 10W portable jammer can be effective across a 30km radius

GAJT reduces the 30km effective range to approximately 230m. Remember that it's highly likely there will be GNSS data feedback on the jammer before it becomes wholly effective

FORSBERG
POSITIONING | NAVIGATION | TIMING

Jammers
Frequencies and Effective Ranges

FORSBERG
POSITIONING | NAVIGATION | TIMING

What are the BAD GNSS Challenges?

Key technical specifications:N8B-LG for 0.5W GPS L1 Interferer

Channel	Output port	Frequency range	Average Output
1	LoJack	167-175MHz	27dBm/0.5W
2	CDMA or GSM	851-894 or 925-960MHz	27dBm/0.5W
3	DCS or PCS	1805-1880 or 1920-1990MHz	27dBm/0.5W
4	Wi-Fi 2.4G	2400-2500MHz	27dBm/0.5W
5	4G1 LTE	700-803 or 790-862MHz	27dBm/0.5W
6	**GPSL1**	**1570-1580MHz**	**27dBm/0.5W**
7	3G	2110-2170MHz	27dBm/0.5W
8	4G Wimax	2500-2690 or 2300-2400MHz	27dBm/0.5W

Power supply: AC adapter 50 to 60Hz, (110-240V AC to 12V DC) Car Charger DC12V
Dimensions: (length, width, height) 132x80x41mm (not include antenna)
Packing size: 220x202x65mm Net weight: 0.6kg Gross weight: 0.8kg Total Power 4W
Shielding radius: (2-20) meters at -75dBm, still depends on the strength signal in given area

Built-in battery:7.4V/4700mAh,Continue working: more than 1.5+ hours.
Warranty: one year from delivery date.

FORSBERG
POSITIONING | NAVIGATION | TIMING

...And the Ugly GNSS Challenges?

Key technical specifications:X16PLUS A for 4W on GPS L1, L2, L3 (NUDET), L4 (R&D) and L5 Interferers

Order information :
X16PLUS A: CDMA/GSM/3G/4GLTE Cellphone/Wi-Fi2.4G/Bluetooth/Walkie-Talkie/Lojack/GPSL1-L5/RC433MHz315MHz868MHz

1. GSM850MHz:850-894MHz; 8W
2.GSM900 925-960MHZ 8w
3. GSM1900MHz or 1800:1805-1880/1920-1990MHz;8W
(2GGSM/CDMA/PCS1900/1800MHz)
4. 3G2100MHz:2100-2170MHz;3W (3GUMTS/WCDMA/TD-SCDMA/CDMA) 8W
5. 4GLTE700MHz:700-803 or 790-862MHz; 8W
6. 4G LTE1700 : 1700-1800MHz 8W
7. 4G Wimax 2500-2690 or 2300-2400MHz 8W
8. Wi-Fi/Bluetooth2.4G:2400-2500MHz; 8W
9. GPSL1 1570-1580MHz 4w
10. GPSL2+L5 1170-1280MHz 4w
11. GPSL3+L4 1370-1390MHz 4w
12. LOJACK 167-175MHz 5W
13. VHF 135-174MHz 5W
14. UHF 400-470MHz 5w
15. RC433 430-440MHz 5w
16. RC315 310-320MHz 5w
Total Output Power: 96W

FORSBERG
POSITIONING | NAVIGATION | TIMING

What are the GNSS Frequencies you lose?

Points 9-11 of the specification are “ugly”

9. GPSL1 1570-1580MHz 4w
10. GPSL2+L5 1170-1280MHz 4w
11. GPSL3+L4 1370-1390MHz 4w

This jammer can simultaneously transmit on all GNSS signals except GLONASS L1 and BEIDOU B1. L band and IRNSS S band are clear too.

However if you completely overpower the receiver it is normal for all signals to be lost*

**Some receivers with in-band filters can work beyond this point. e.g. NovAtel ITK and Septentrio AIM+*

GPS		GLONASS		GALILEO		BEIDOU		SBAS		L band		IRNSS		MSAS		QZSS	
L1	1575.420	**L1**	**1593-1610**	E1	1575.420	**B1**	**1561.098**	L1	1575.420	**L**	**1525-1560**	L5	1176.45	L1	1575.42	QZS-L1-CA	1575.42
L2	1227.600	L2	1237-1253	E5a	1176.450	B2	1207.140					S	2492.028			QZS-L1-C	1575.42
L5	1176.450	L3	1192-1210	E5	1191.795	B3	1268.520	L5	1176.450							QZS-L1-SAIF	1575.42
				E5b	1207.140											QZS-L2C	1227.60
				E6	1278.750											QZS-L5	1176.45
																LEX	1278.75

At what Distance does GNSS lose Positioning when Jammed?

Loss of Positioning - Range from Jammer in Metres

	Watts	Poor + a/j	Poor	OK + a/j	OK	Good + a/j	Good
	10.49	384m	49152m	192m	24576m	96m	12288m
The UGLY	**4.02**	**238m**	**30440m**	**119m**	**15220m**	**59m**	**7610m**
	2.62	192m	24576m	96m	12288m	48m	6144m
	0.66	96m	12288m	48m	6144m	24m	3072m
The Bad	**0.50**	**84m**	**10772m**	**42m**	**5386m**	**21m**	**2700m**
	0.16	48m	6144m	24m	3072m	12m	1540m
The Good	**0.010**	**12m**	**1536m**	**6m**	**768m**	**3m**	**384m**
	0.00001	**<1m**	**48m**	**<1m**	**24m**	**<1m**	**12m**

a/j refers to a digital anti-jam antenna such as GAJT. However even that small amount of power from NEAT highlighted as GOOD (because only certified people operate them) denies GNSS positioning over quite large areas. Increase the power and the radius of denied GPS operation gets worse for not a lot more battery power.

Jammer Protection
Anti-Jam Antenna

FORSBERG
POSITIONING | NAVIGATION | TIMING

Forsberg Provides GPS Protection Equipment

GAJT-710MS Mount

FSL custom mounting option for the GAJT-710MS which provides:

- Power management (AC and DC inputs)
- Cable management
- Mounting to Type 26 ship structure
- Corrosion resistant
- RF amplification for long cable runs

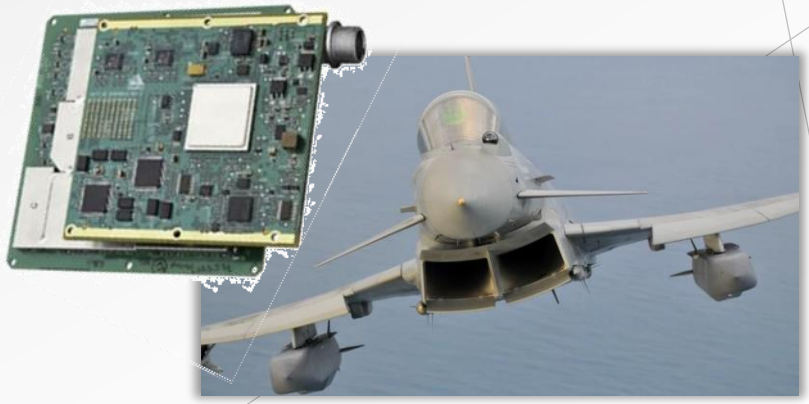
Q. Why are they relatively expensive?
A. Because they sell in low numbers and are costly to develop and support.

Q. Can I use them?
A. Yes, but you need an export licence because countries control their use.

GAJT-AE Ruggedised Enclosure

Anti-jam system for a defence program. We use the core processing cards from the GAJT, some of our own StarLink RF "special" products and a custom PCB.

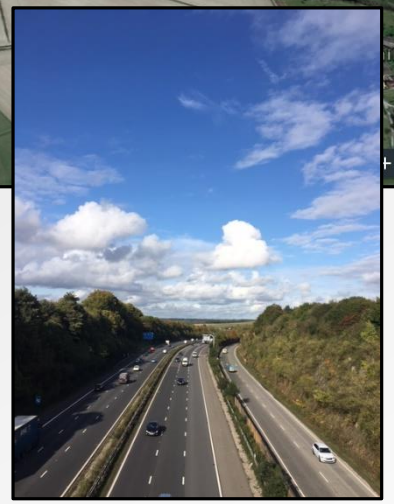
The whole system is designed to survive extreme environmental conditions while satisfying the platform navigation interface requirements.

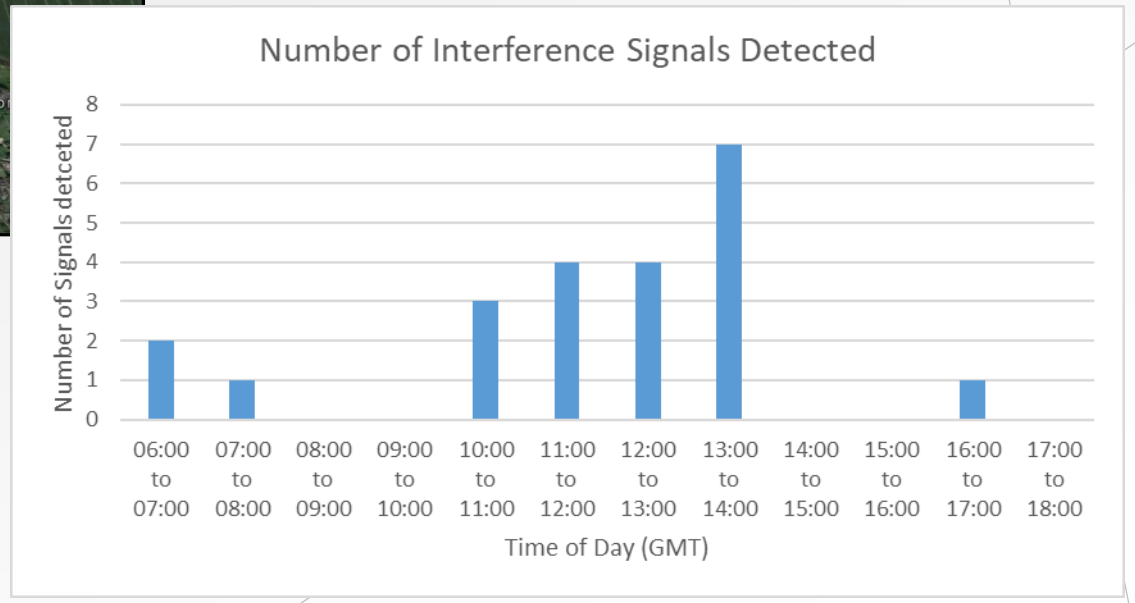


FORSBERG
POSITIONING | NAVIGATION | TIMING

Jammers
What do we Know?

Jamming Survey – Roads





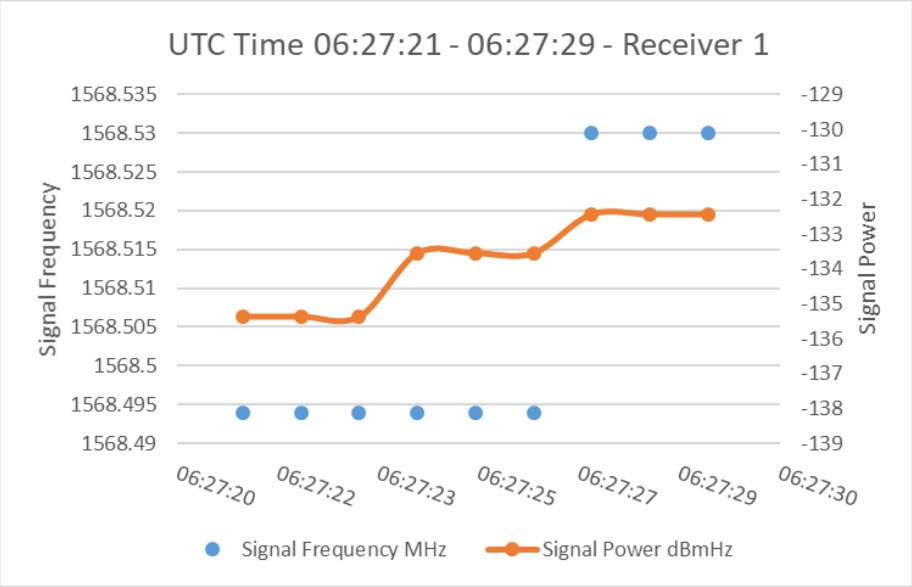
Relatively high number of detections on a motorway (snelweg). 22 detections over eleven hours. Most (12) in the middle of the day

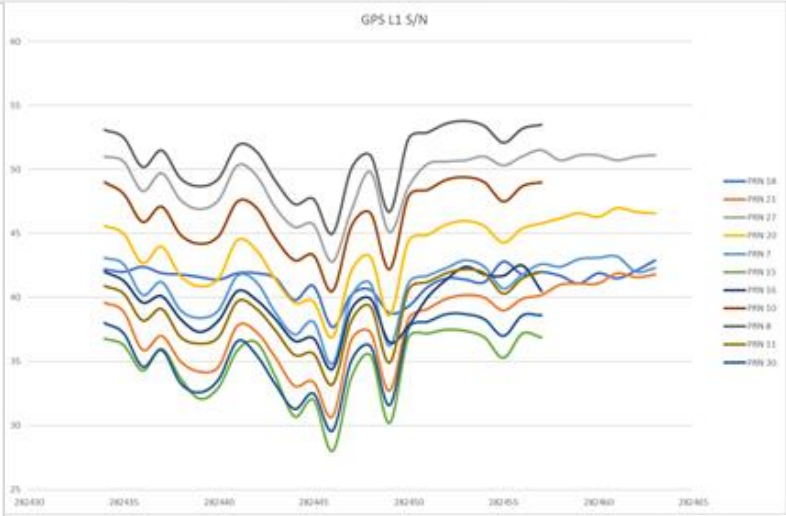
FORSBERG
POSITIONING | NAVIGATION | TIMING

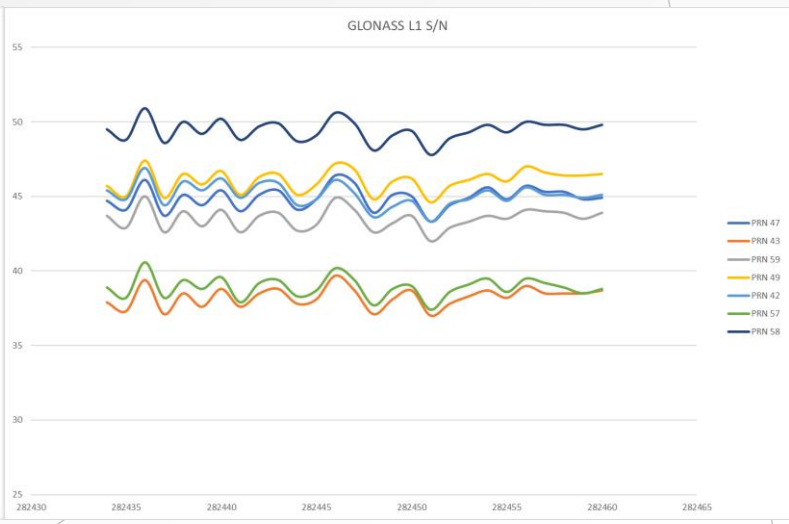
WWW.FORSBERGPNT.COM

Jamming Survey

- The interference noise is mild and degraded but didn't stop navigation.
- Black market GNSS jammers are inconsistent in build quality. Out of 22 detections in an eleven hour period we noted that almost all of them were close to rather than on the GPS L1 C/A code frequency of 1575.42 +/-1.023MHz and GLONASS L1 code frequency of 1593-1610 MHz. (Left-hand graph)
- Because they are off frequency they're not as effective as they could be, and we could place a filter over the noise and still read the signal.
- AGC adjusted gain for eleven GPS satellites during an event (Middle) shows the gain dip as the jammer transits past. Notice that GLONASS (right) does not dip in the same way.



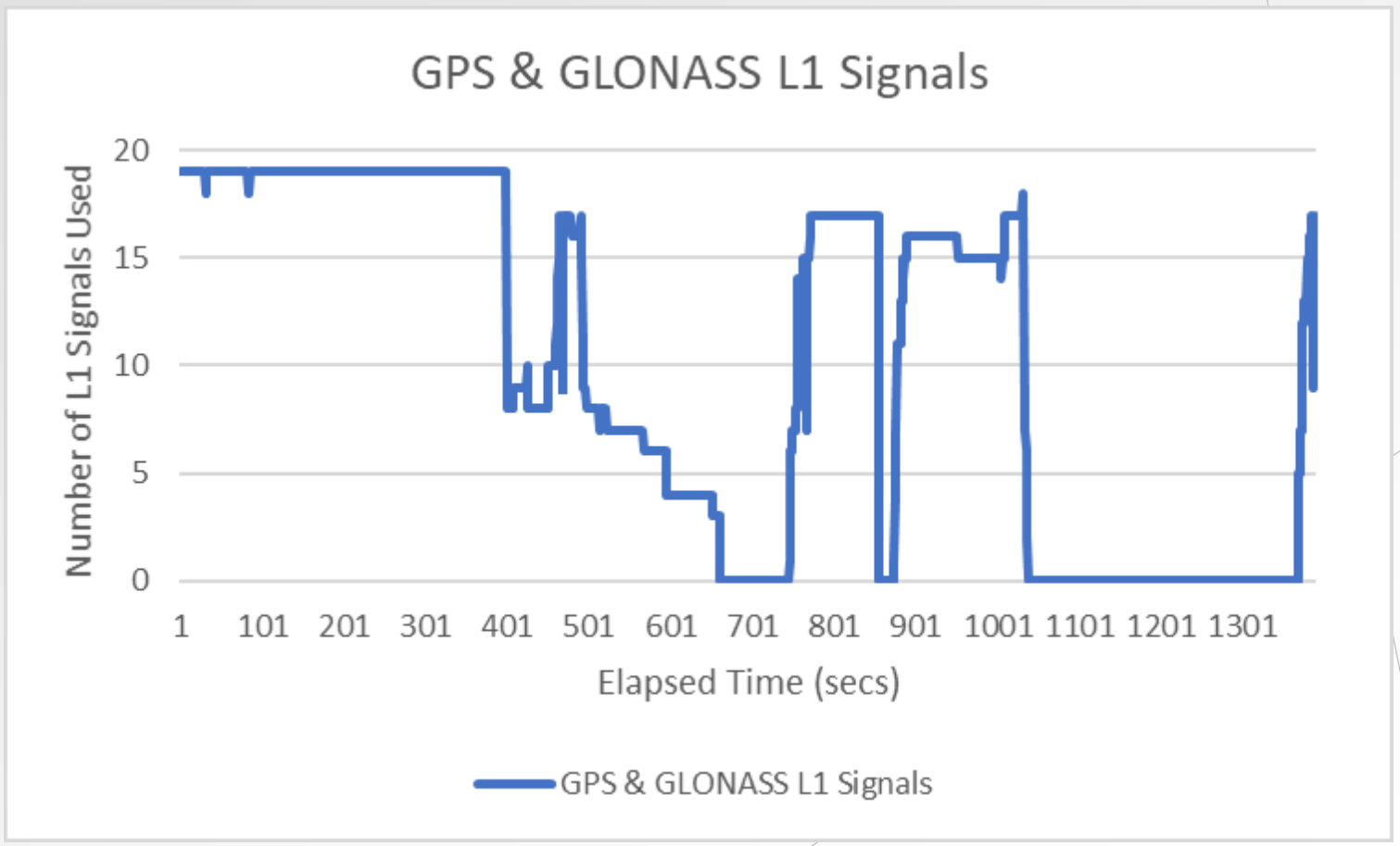




FORSBERG
POSITIONING | NAVIGATION | TIMING

Jamming Survey – A Strong 1W GPS L1 Jammer did this

- Jamming occurs only on the GPS L1 frequency
- From 0-400 seconds there is no (or limited) jamming. The receiver outputs positions.
- From 650-750 seconds jamming is massive – It's on the GPS L1 frequency but GLONASS is lost too.
- From 750 seconds onwards the jammer power is adjusted and positioning starts to recover. At 850-860 and 1050-1390 seconds max. power is applied again.
- From 750-1050 we also had RTK (position and heading) except for 850-880 seconds.
- Most L2 signals were also lost due to use of L1 based codeless tracking.



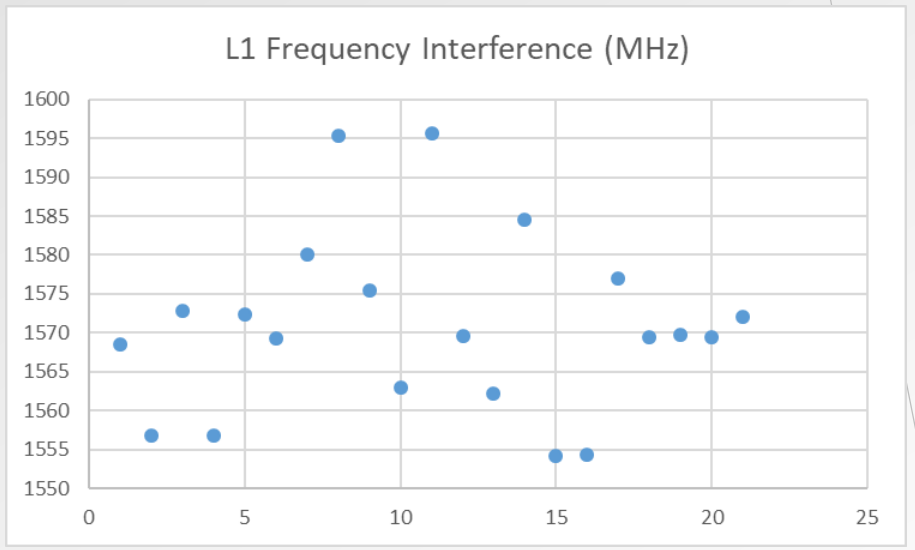
FORSBERG
POSITIONING | NAVIGATION | TIMING

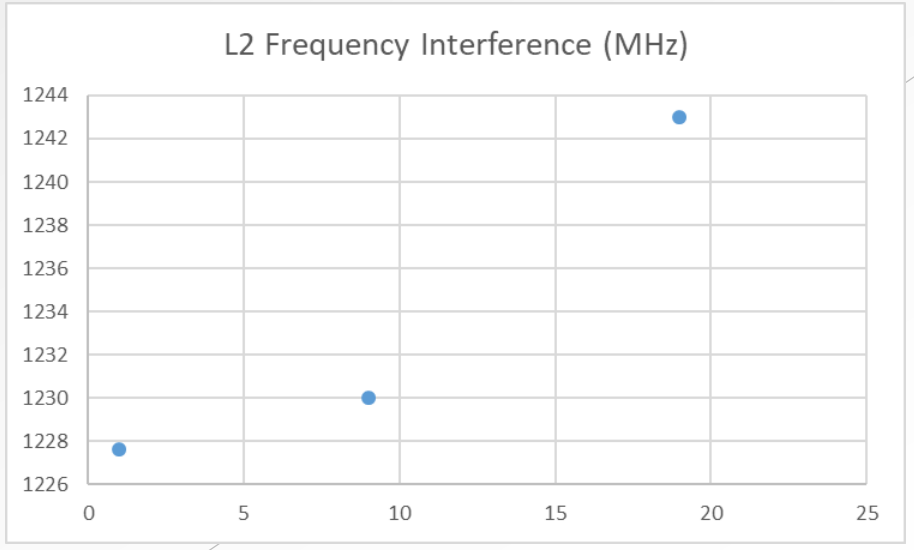
What is there to Like about jammers?

"Internet purchased" Jammers are often off-frequency. This does reduce jammer effectiveness.

Note the one hit on the correct frequency L1 #12 and a second on L2 #1. Arguably you should lose navigation if there's an interference event between 1563 and 1588MHz. However we have tested significant interference within this band filtered it out and continued to navigate on receivers we have tested.

Also note the predominance of L1 only events. Only three incidents involved L2 and one of those had no matching L1 interference. Jamming GPS L2 didn't stop our receivers working until it was so powerful that the L2 band was saturated rendering the receiver incapable of reading any signal.

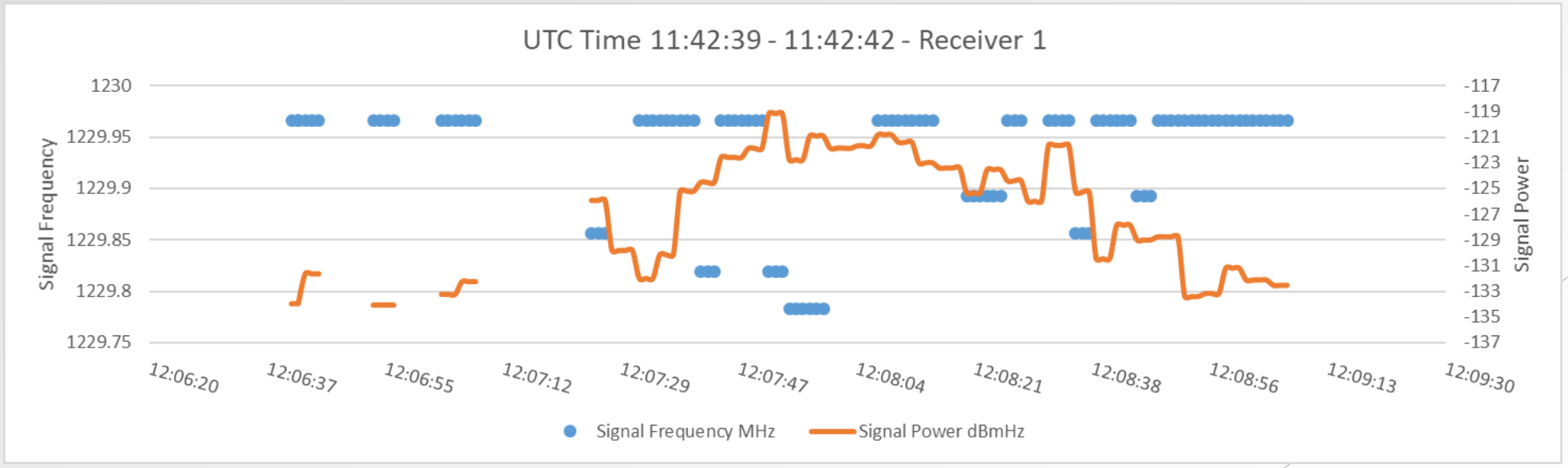




FORSBERG
POSITIONING | NAVIGATION | TIMING

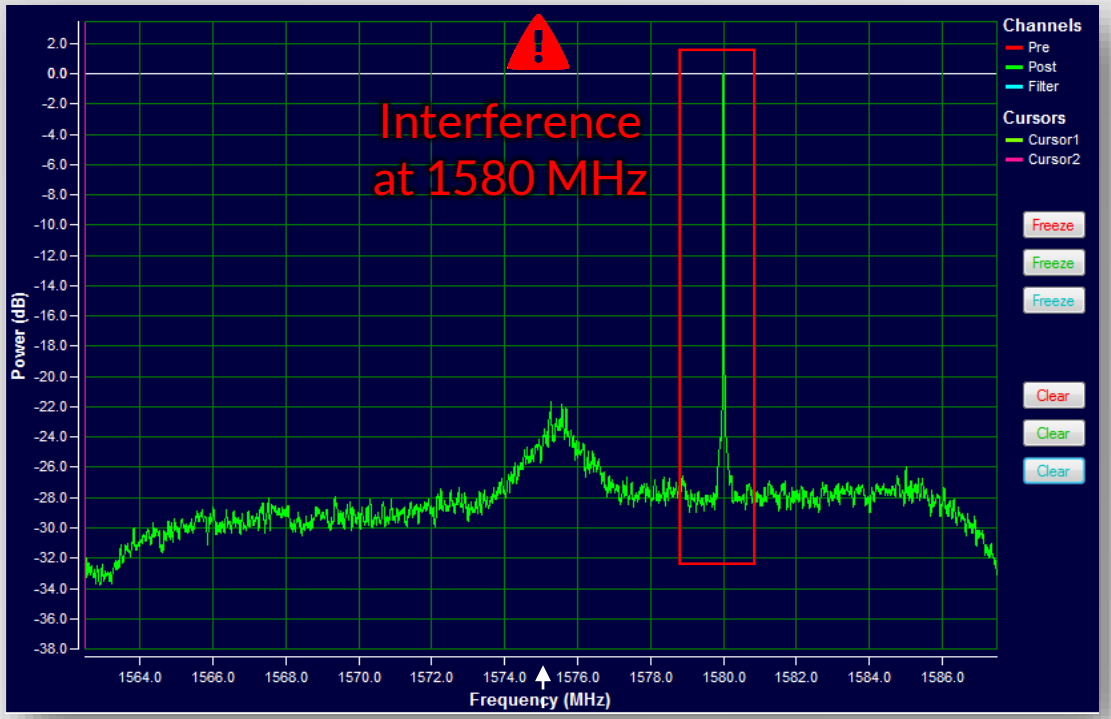
What is there to Like about jammers?

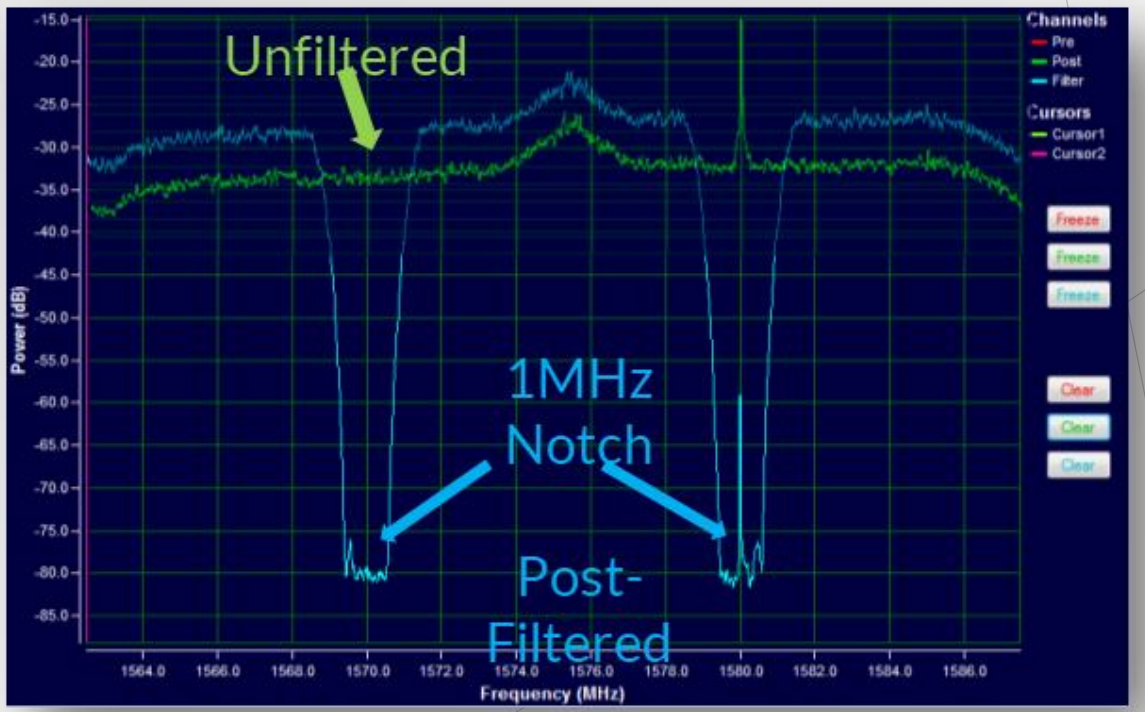
We like L2 jammers because it doesn't do any real harm to a C/A code receiver until significantly more powerful signals are transmitted. This prolonged event was close to L2 and not L1. It didn't affect L1 navigation. The prolonged interference over 2.5 minutes took the jammer behind obstructions. It was also off frequency. No L1 interference was detected. Why was it only on L2? Maybe the jammer malfunctioned.



ATTENUATE INTERFERENCE WITH ITK MITIGATION FEATURES

The left plot shows what a 28dB interference signal looks like at 1580MHz. The small bump to the left of the narrow-band spike is the GPS L1 signal. In the right-hand plot's blue trace we have filtered the spike out and continued to navigate.



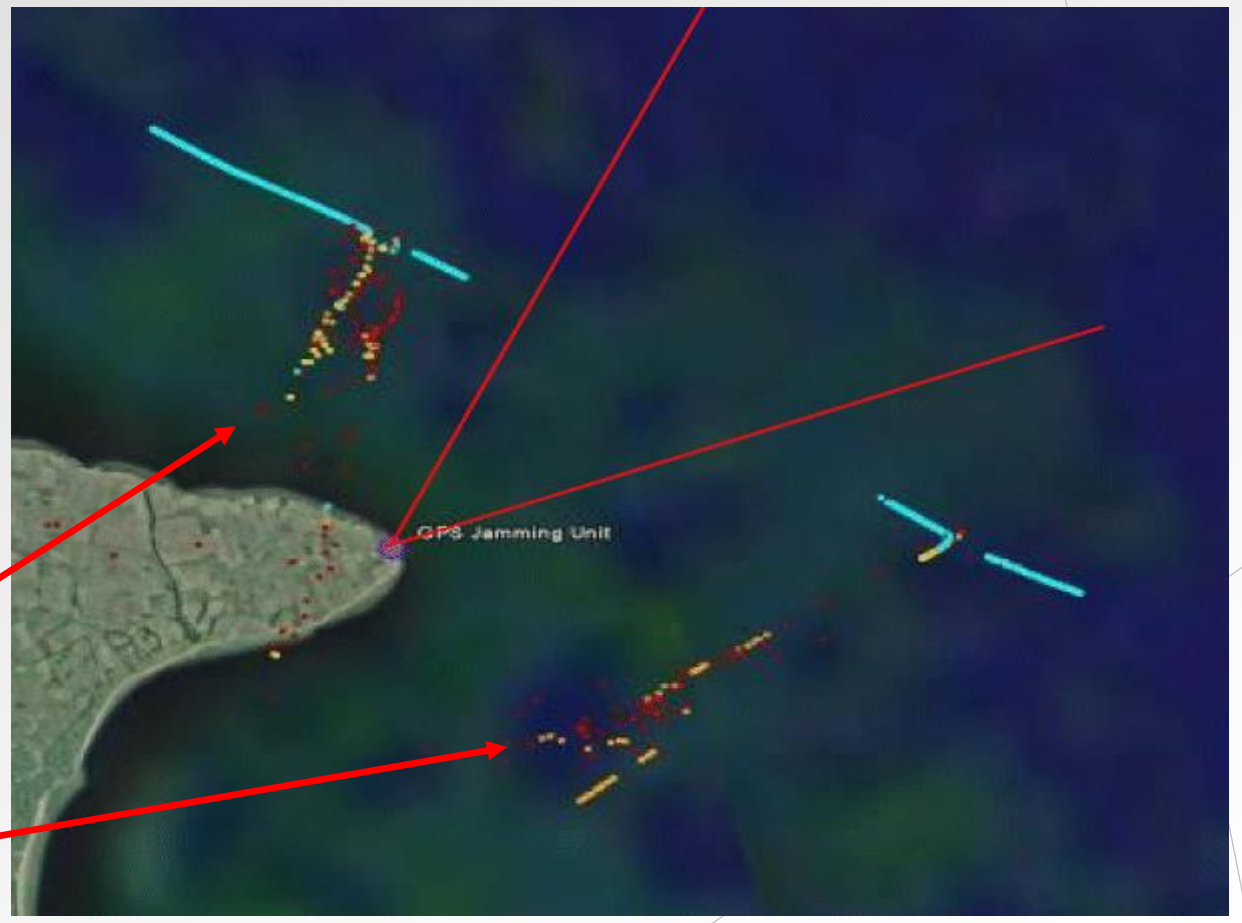


FORSBERG
POSITIONING | NAVIGATION | TIMING

Jamming Threat at Sea – Trinity House Trial

Trinity House:
GALATEA

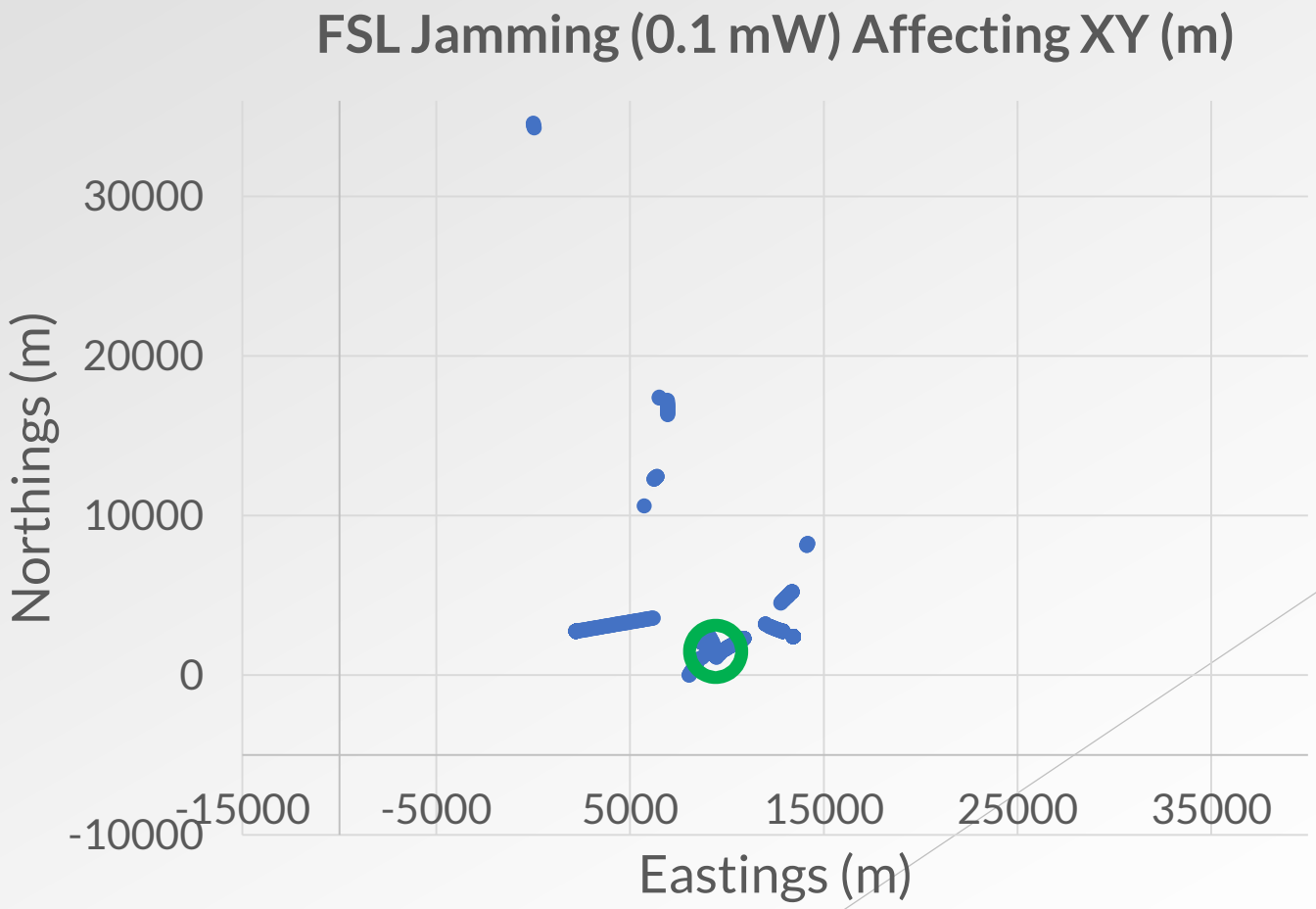
The report tells us that no spoofing was used yet the ship's positions moved miles away from the correct positions.



2011 *UK jamming trials: hazardous and dangerous effects before total loss of PNT.*

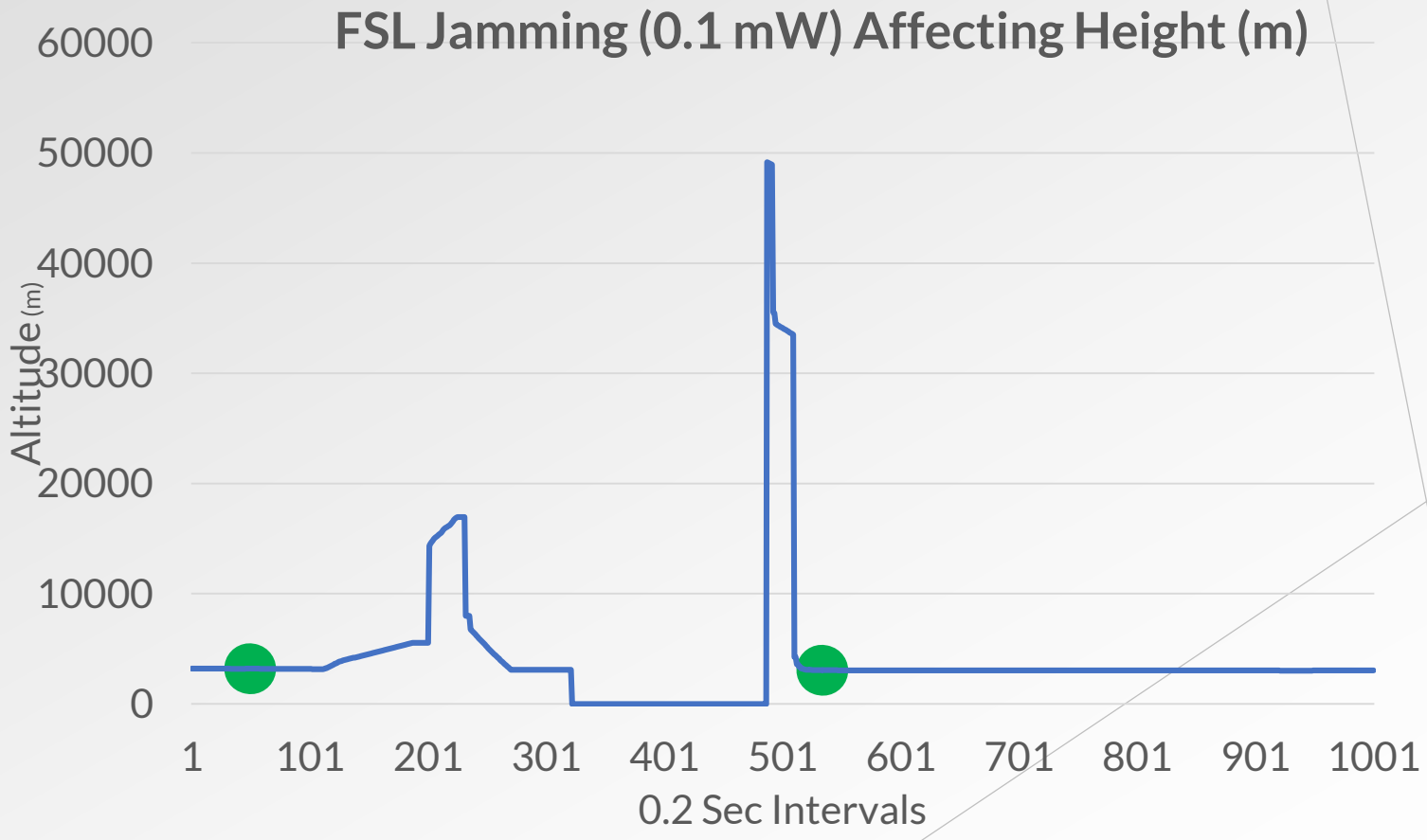
Confirmation that Jamming can cause Bad Positions (1)

- Horizontal displacement of 35km
- Jamming - Yes
- Spoofing – None
- GNSS Receiver Quality - Poor

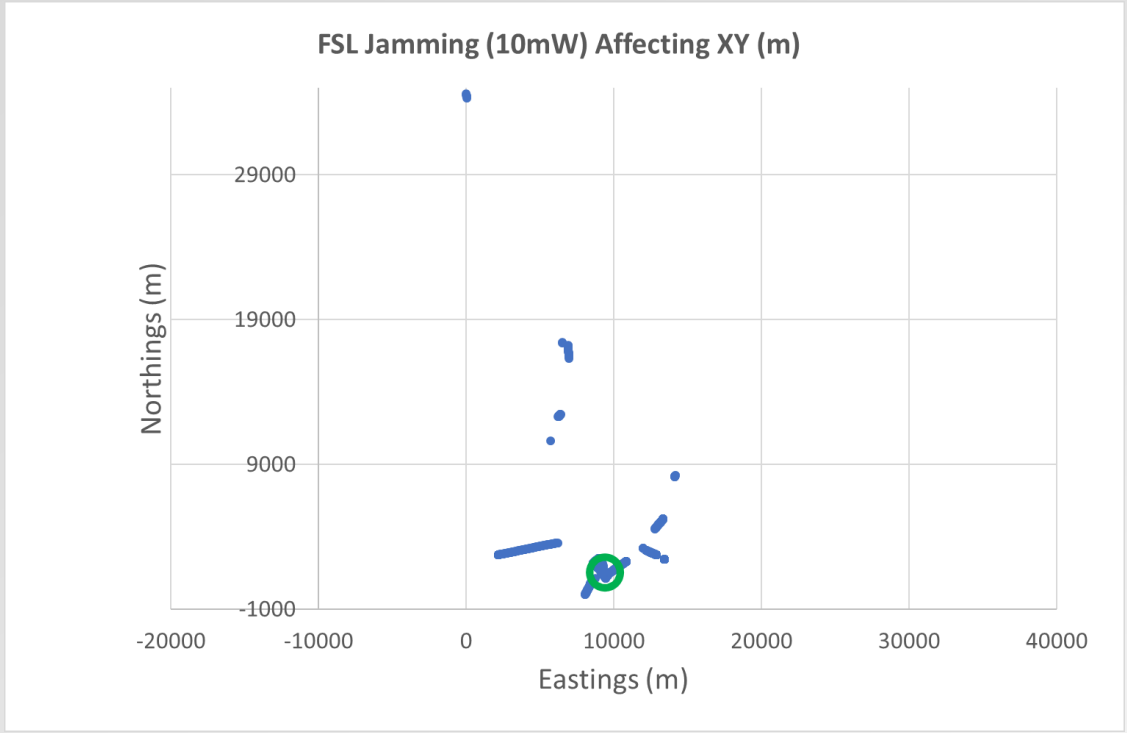


Confirmation that Jamming can cause Bad Positions (2)

- Vertical displacement of 50km
- Jamming - Yes
- Spoofing – None
- GNSS Receiver Quality - Poor

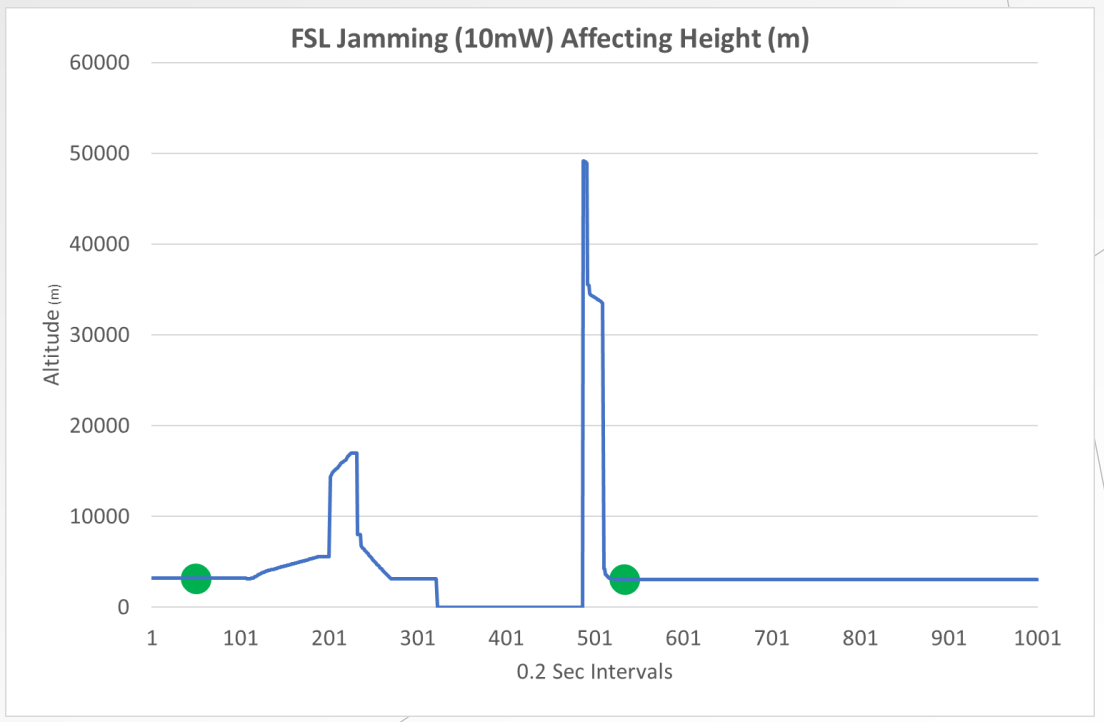


Confirmation that Jamming can cause Bad Positions (3)



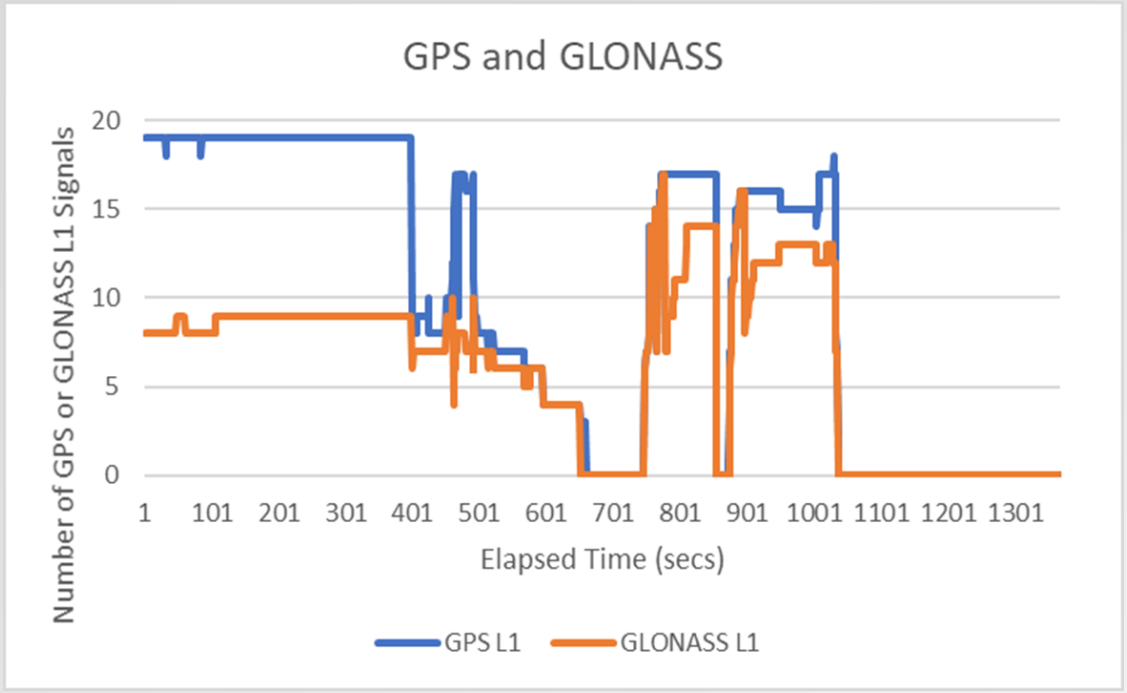
This receiver was actually moving at about 3 kph but apparently travelled out ~80km and back in 40 seconds. That was an average of ~14,400 kph. (COCOM Limits?)

This poor quality GNSS receiver didn't just stop positioning it also self-spoofed its position for ~40 seconds. We suspect some predictive tracking. Two possible causes are a MEMS sensor and/or the signal processing? Investigation is ongoing

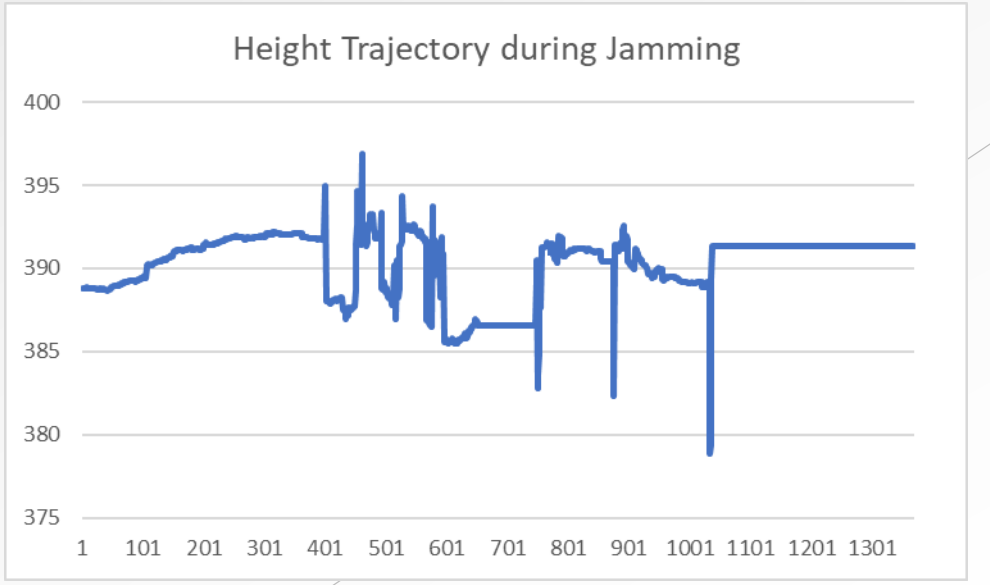


FORSBERG
POSITIONING | NAVIGATION | TIMING

Confirmation that Jamming can cause Bad Positions (4)



This good quality GNSS receiver is predictable. It did not self-spoof. It also didn't show much variation in position as it was jammed. This is what a user would probably want to happen.



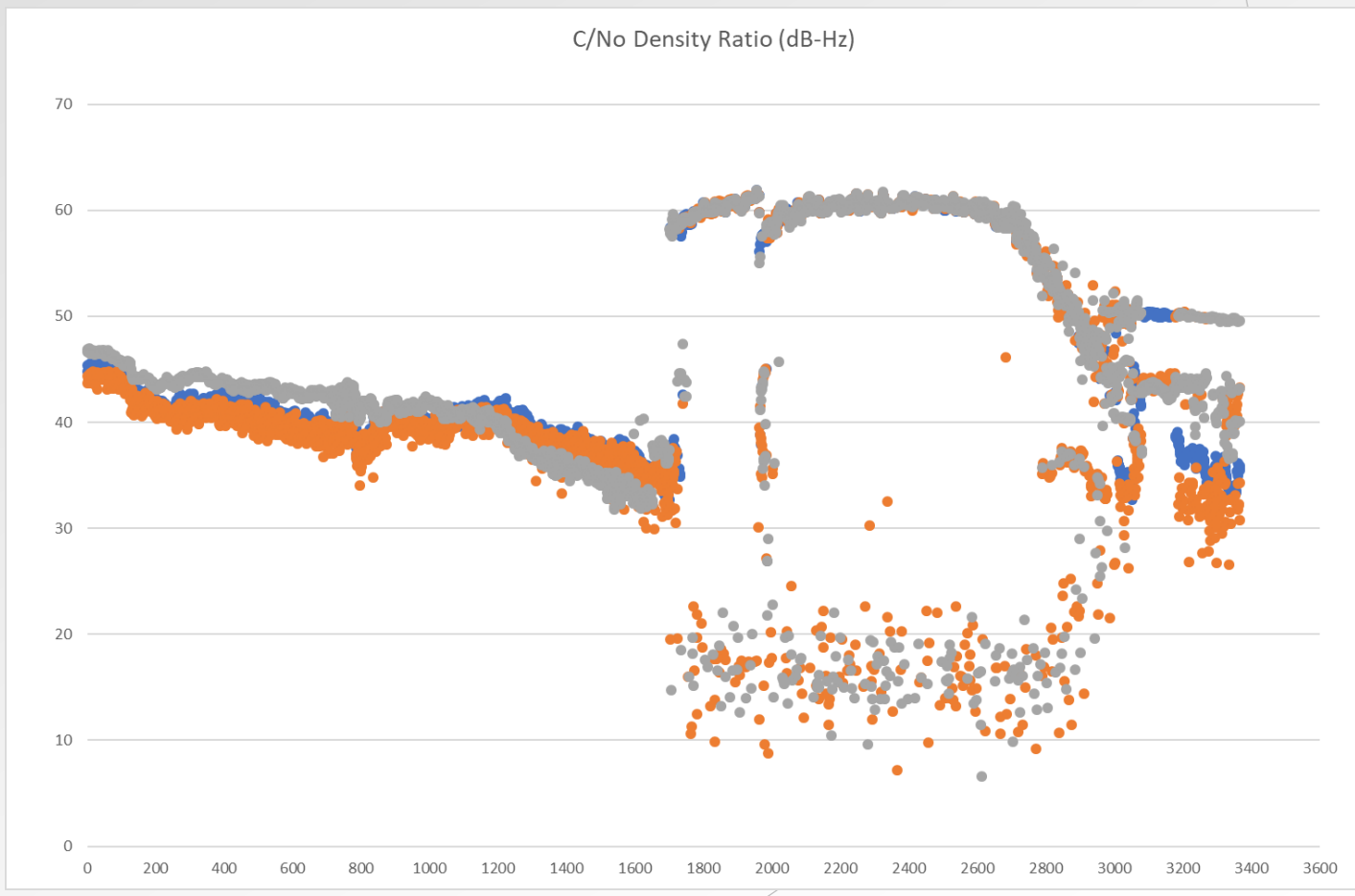
This receiver was stationary but froze its position when jammed between 380 and 1300 seconds. Positioning continued but the good quality GNSS receiver correctly reported the positions as poor.

FORSBERG
POSITIONING | NAVIGATION | TIMING

Spoofers
What do we Know?

What we saw in a GPS-only Spoofing Trial (1)

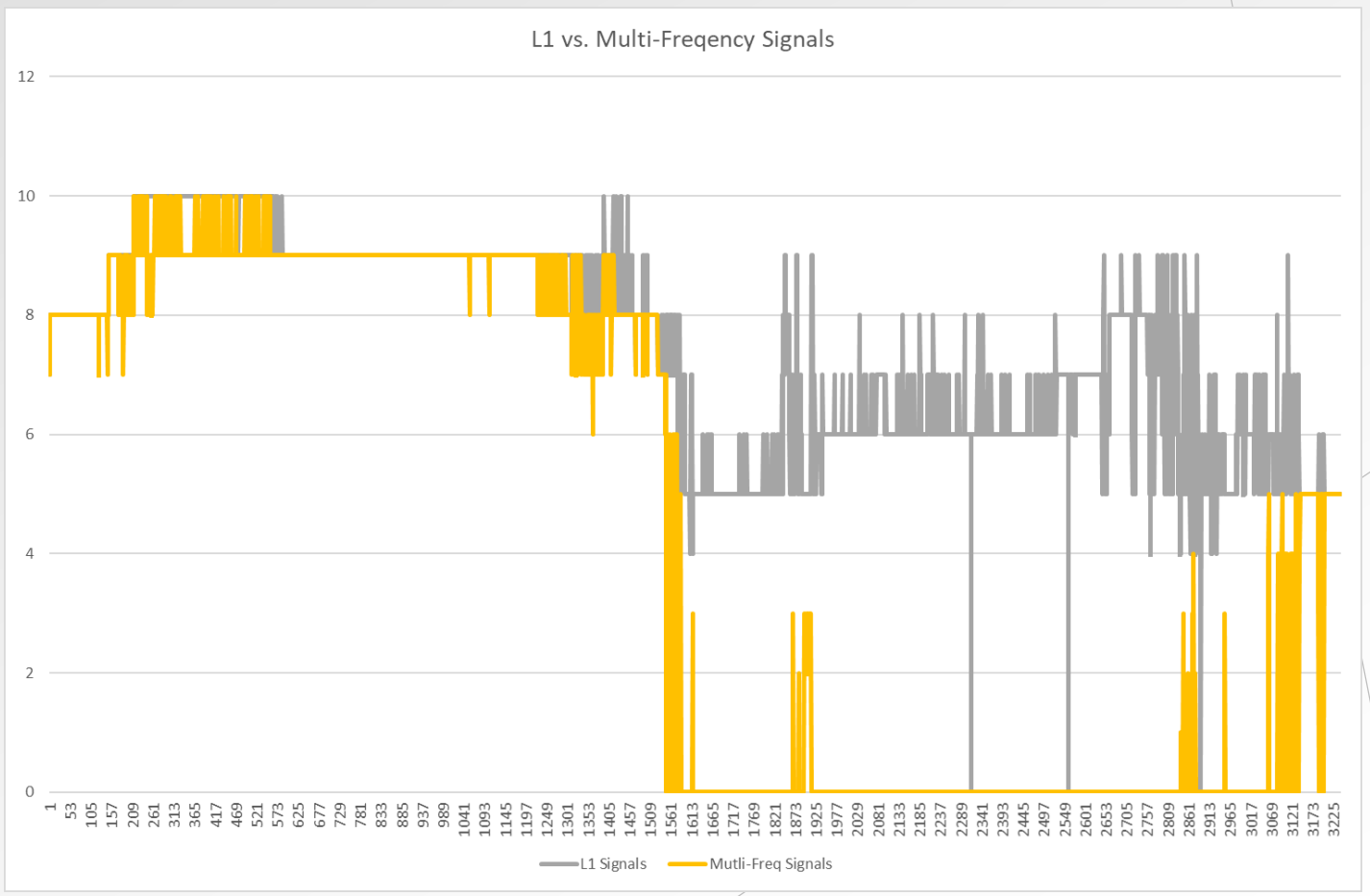
- We used a good quality GPS Rx
- We first saw jamming of the GPS Signals
  - First failed attempt at 800 seconds
  - Massive successful attempt at 1670 seconds
- C/No values for three satellites sampled
  - 0-1670 seconds fairly normal values
  - 1670-2700 all satellites show the same C/No
  - 2700-3100 increasingly credible C/No values
  - 3150-3400 true signal begins to break through
- This was very hard to achieve
  - Used a GPS Simulator to generate signals
  - Spoofed GPS RX remained static throughout
  - Signal power was hard to adjust
  - Adjusting power level for spoofer to convincingly control the GPS RX is difficult even though we know where the RX is and that it's stationary. True GPS satellites started to break through once the spoofed C/No became believable.



FORSBERG
POSITIONING | NAVIGATION | TIMING

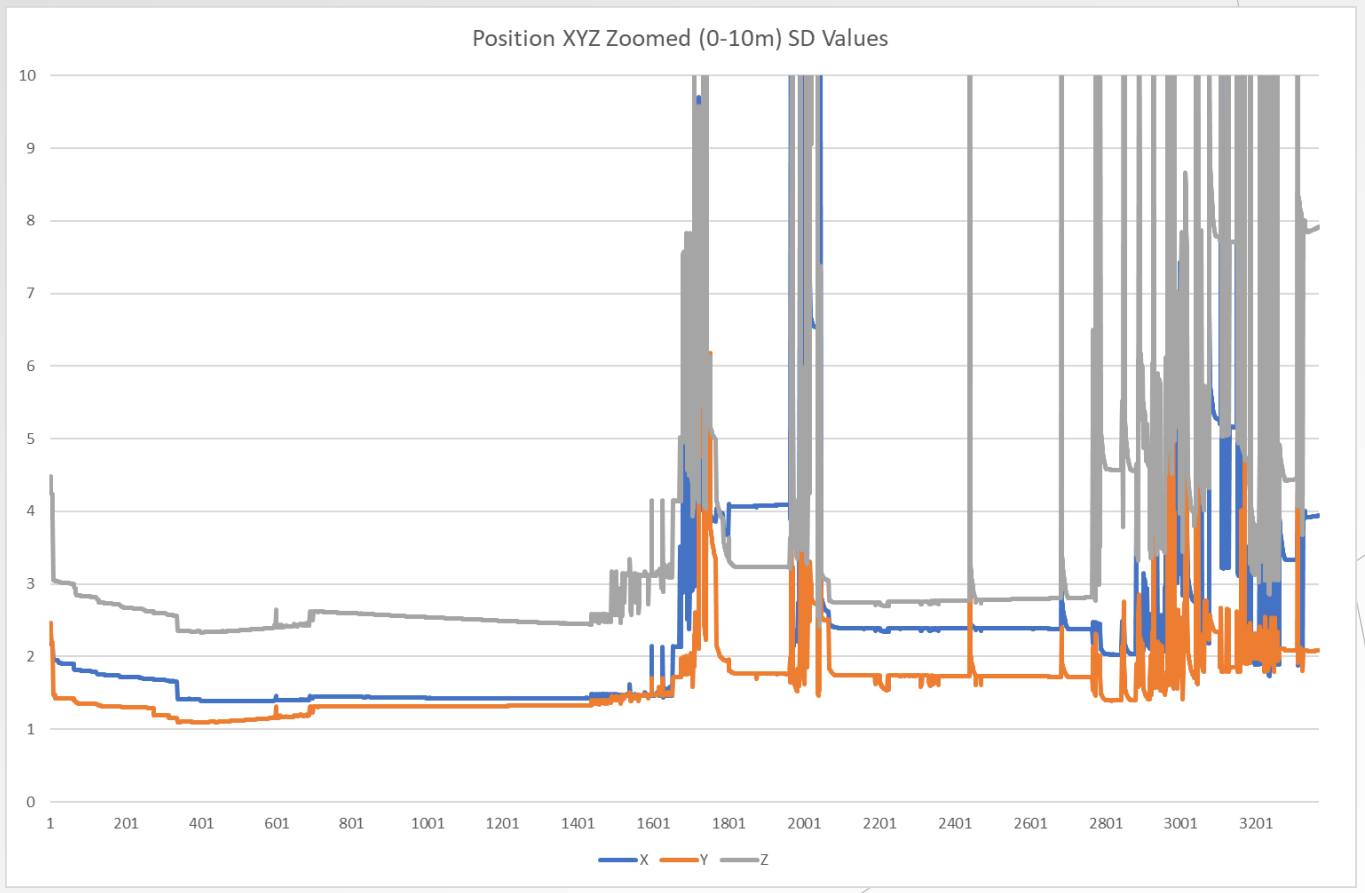
What we saw in a GPS-only Spoofing Trial (2)

- We used a good quality GPS Rx
- **We saw Satellite numbers change**
  - **Up to 1200 L1 and L2 signal numbers matched**
  - **After 1200 very few L2 signals (jamming & spoofing)**
  - **After 3000 L2 signals start to be picked up (corresponds to breakthrough of genuine L1 signals)**
- **This is abnormal**
  - **Why would be normally lose everything except L1 signals? We wouldn't**
  - **Satellite Signals were erratic for no good reason**



What we saw in a GPS-only Spoofing Trial (3)

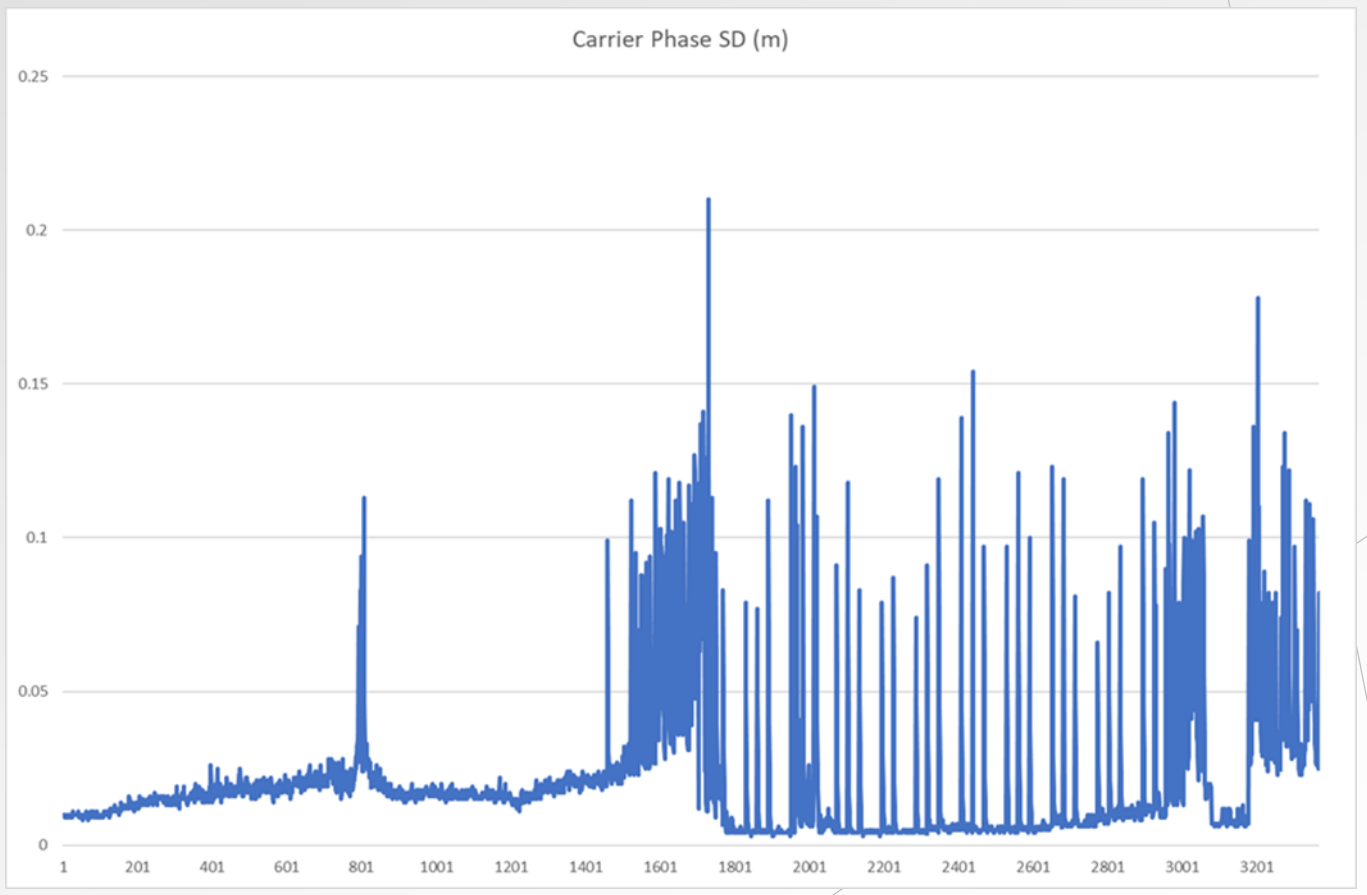
- We used a good quality GPS Rx
- **We saw Position Accuracy Vary**
  - At 1600 Jamming and Spoofing started
  - Up to 1400 seconds accuracy looked believable
  - After 1400 seconds Y accuracy becomes worse than Z accuracy !
  - Increasingly erratic
- **This is abnormal**
  - We rarely see Y accuracy worse than Z accuracy
  - There was no obvious reason for the varying accuracy



FORSBERG
POSITIONING | NAVIGATION | TIMING

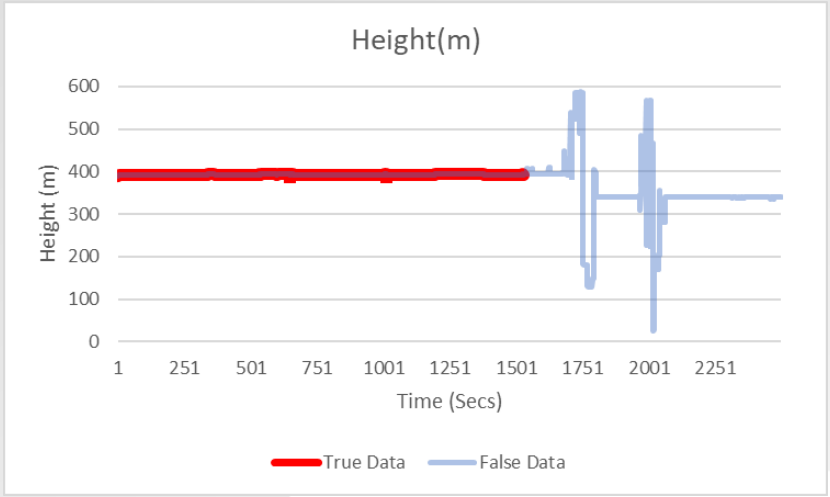
What we saw in a GPS-only Spoofing Trial (4)

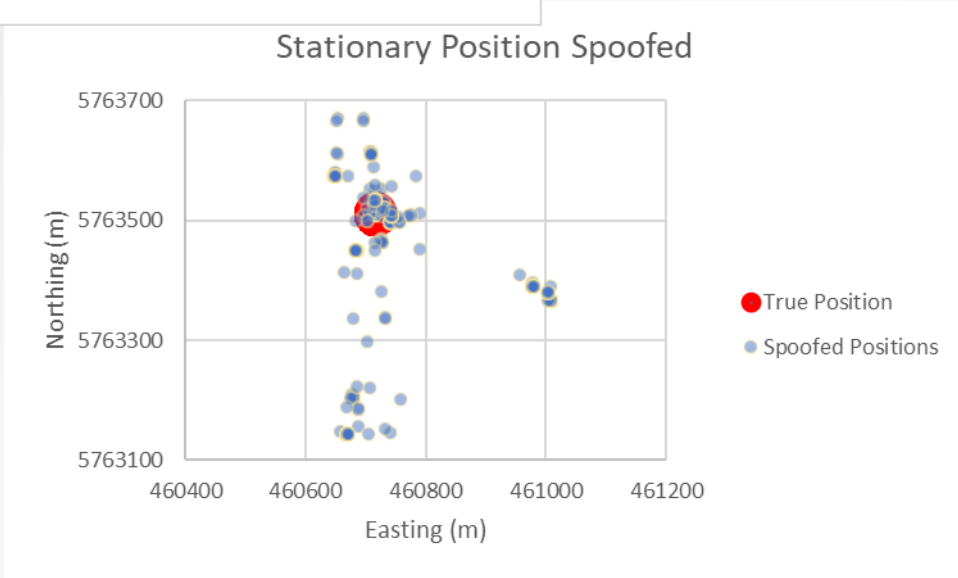
- We used a good quality GPS Rx
- **We saw Carrier Phase SD vary**
  - **At 800 Jamming and Spoofing failed but upset the carrier phase SD value**
  - **Otherwise up to 1400 seconds precision and quality looked believable**
  - **After 1400 seconds carrier phase SD became erratic. On occasions it was very good (too good) and often it was very bad.**
- **This is abnormal**
  - **Apart from 0-1400 secs (excl. 800) the data is highly irregular. Both very good and very bad carrier phase SD values are experienced.**



What we saw in a GPS-only Spoofing Trial (5)

- We used a good quality GPS Rx
- **Our Findings**
  - **Spoofing is identified by many values and events**
    - **Position accuracy**
    - **Signal Strength**
    - **Satellite numbers**
    - **Measurement precision**
    - **…**
- **Recommendations**
  - **Examine normal data and characterise it**
  - **Run continuous tests and query non-standard data**
  - **Use a receiver providing more than simple NMEA**
  - **Consistently use multiple modes of navigation**
- **Conclusion**
  - **Spoofing is identifiable and avoidable**
  - **Commercial receivers can be resistant to spoofing by thorough data analysis**
  - **Slides 26-28 showed some receivers to self-spoof**





Contact Details

Forsberg
North Quay, Heysham Port, LA3 2XF

+44 (0)1524 -383320
info@forsbergpnt.com
www.forsbergpnt.com

Company Registration: SC104949