MULTI-SITE MULTI-BAND GNSS INTERFERENCE MONITORING AND ALERTING

Aiden Morrison, 12.10.2020

Today's Schedule

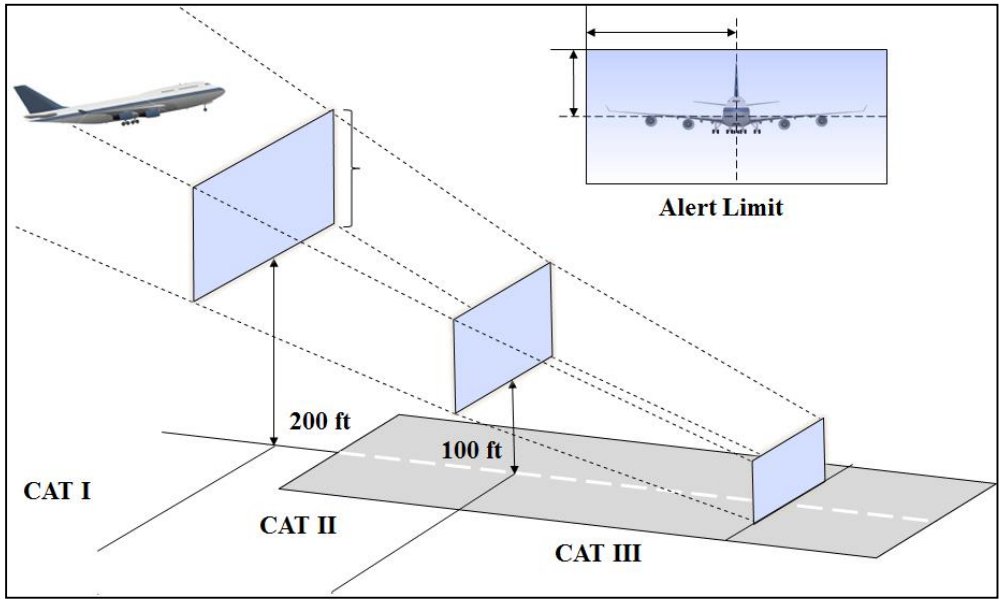
- Introduction
- Background and motivation
- The Advanced RFI Detection, Alerting and Analysis System (ARFIDAAS) project
  - Deployment, and results
- Future plans
- Honorable mentions
  - Manufacturers say the funniest things about jamming/spoofing
  - ’Secure’ signals may not be as secure as we might hope
- Conclusions

SINTEF Navigation team introduction

		
Nadia Sokolova: Specialist on GNSS augmentation systems and high integrity navigation. 14 years experience.	Aiden Morrison: Specialist on navigation sensor system development. 13 years experience.	Are Hellandsvik: Specialist on embedded electronics and communications systems. 18 years experience.

- This is the core GNSS group
  - Other members of the connectivity technologies and platforms department join as needed
  - Next – background and motivation

Background/Motivation 1: GBAS assumptions



GBAS Precision Operation		CAT I	CAT II	CAT III
Accuracy [m] 95 %	Horizontal	16.0	6.9	6.1
	Vertical	7.7	2.0	2.0
Integrity	Time-to-Alert [s]	3	2	2
	Alert Limit [m]	H: 40 V: 10-15	H: 17.3 V: 5.3	H: 15.5 V: 5.3
	P_{HMI} / approach	$2x10^{-5}$	$2x10^{-9}$	**$2x10^{-9}$**
Continuity	Failure Rate	$5x10^{-5}$ / approach	$5x10^{-6}$ / 15 sec	**10^{-7} / 15 sec**
Availability		0.99 – 0.99999	0.99 – 0.99999	**0.99 – 0.99999**

- GBAS has the advantage of using multiple ground antennas but RFI at even 1 antenna can reduce availability unacceptably
  - We have observed multiple instances of jamming in Trondheim strong enough to be simultaneously visible to sites **1km apart**
  - Baselines between GBAS receivers are typically <1km
  - Why are jammers so common?

SINTEF

Background/Motivation 2: Public perceptions of jamming

- The way jammers are marketed is troubling
  - People are paranoid about tracking
  - People do not understand the legality
    - Nowhere in the marketing material does it say ‘highly illegal’
  - The advertised range makes it sound like this is a ‘bubble’ around your car

Here is the full list of frequencies which this device is able to work with:

- GSM800 and GSM1900 in USA, GSM900 and GSM1800 in Europe
- CDMA850 in both USA and Europe
- GPS L1, L2 and L5 bands, GLONASS
- WiFi, Bluetooth and all devices operating at 2.4GHz
- 3G frequency

Specifications:

- Working Radius: 15 meters
- Signal Power: 1200mW

www.jammer-store.com

- Even if the 1200 mW is shared between all six bands this is > 1km range

- The propagation environment between the jammer and the victim varies widely
  - Car body can introduce up to 20dB of attenuation in some directions
  - Some jammers have adjustable power levels to compensate

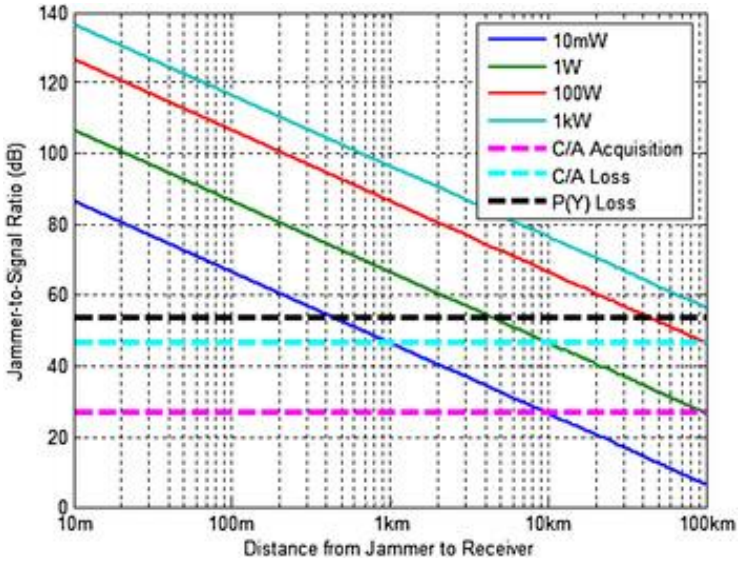


Image from Glomsvoll and Bonenberg

SINTEF

Background/Motivation 3 - growing problem for aviation

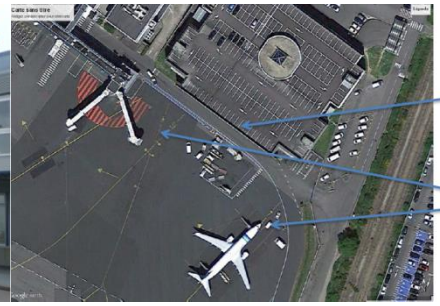
Truck driver has GPS jammer, accidentally jams Newark airport

An engineering firm worker in New Jersey has a GPS jammer so his bosses don't know where he is all the time. However, his route takes him close to Newark airport, and his jammer affects its satellite systems.

BY CHRIS MATYSZCZYK | AUGUST 11, 2013 8:08 AM PDT

JAMMING: Piloter advares mot at GPS-signalet kan forsvinne i luftrommet fra Kirkenes til Lyngen i Troms. Foto: Privat

'Forgotten' GPS jammer costs motorist €2,000



Pilotene mister GPS-signalet i Finnmark. Det kan knyttes til russiske øvelser

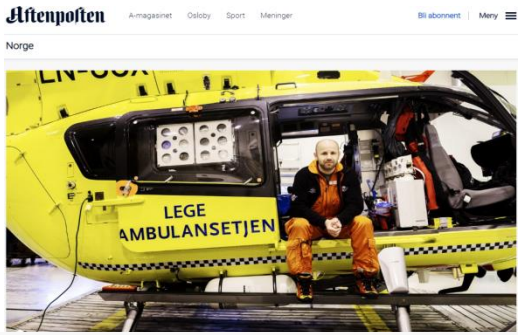
«Det er grunn til å tro at det kan relateres til militære øvelsesaktiviteter utenfor norskekysten», sier Luftfartstilsynet.

'We hacked U.S. drone': Iran claims it electronically hijacked spy aircraft's GPS and tricked aircraft into landing on its soil

By: Craig Mackenzie and Mark Duell
Updated: 10:36 EDT, 19 December 2011

The Chirp Jammer: a GPS hit and run

The €50 device that brought a multi-million euro project to a standstill



Luftambulansen mistet navigasjonssystemet på vei til pasient. Årsaken sto i sigarettenneren til en bil.

Piloten var overlatt til det han så ut vinduet for å finne veien til den kritisk syke pasienten.

GPS Jamming at Cairo

24 MAY, 2016 / DECLAN SELLECK / 3 COMMENTS

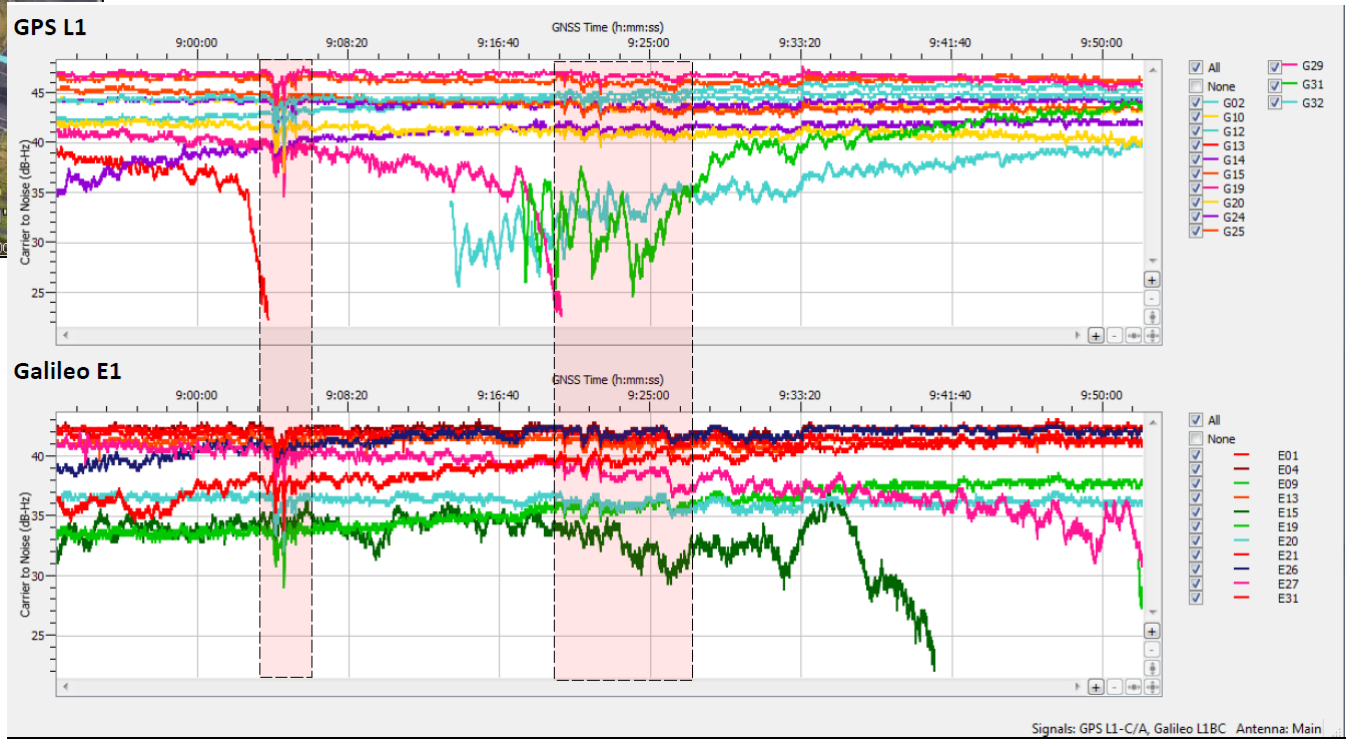
SINTEF

Background/Motivation 4 - Jamming Event at Tenerife Norte

- Experimental GBAS installation (not a full GS, no VDB).
- Installed mid June 2018 as a part of SESAR 2020 PJ 14.3.1 by Indra Navia in cooperation with SINTEF and Enaire.

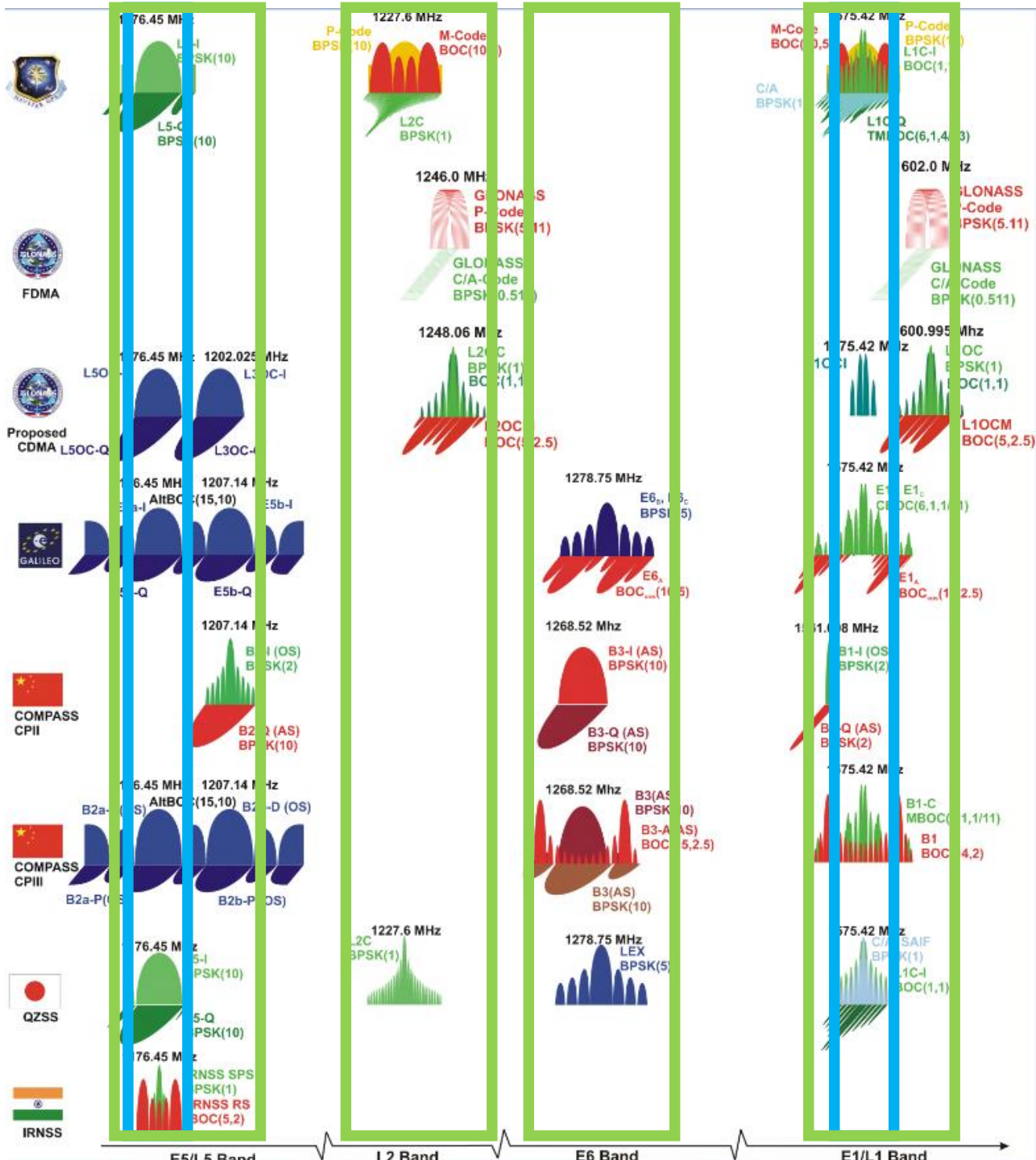
- Each antenna connected to one GBAS receiver (CMA4048) and one COTS DFDC (GPS, Galileo) receiver.
- AR2 is also co-located with a MFMC scintillation monitor.

- Our reaction was the ARFIDAAS project

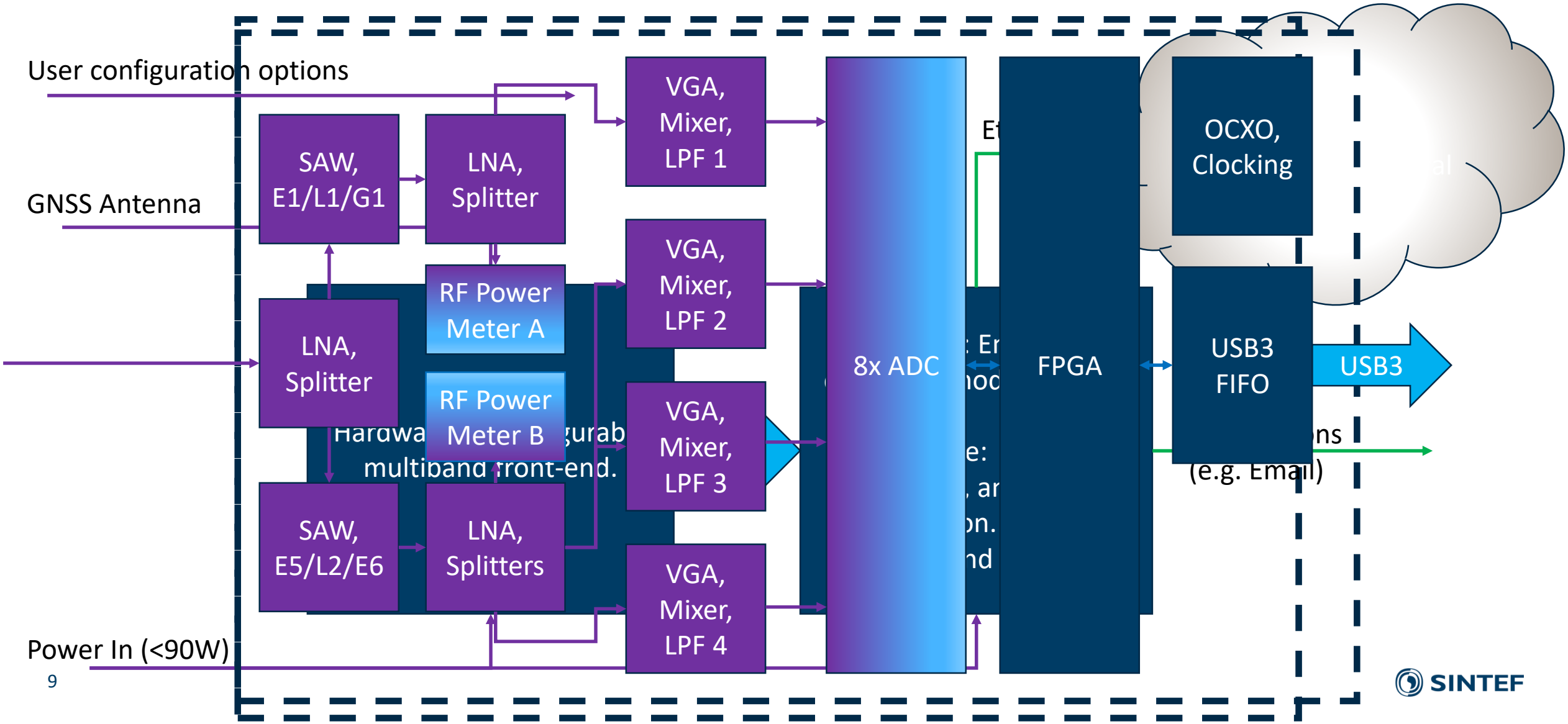


ARFIDAAS 1 - Monitored Bands

- A chart is helpful:
  - Ignoring the S-band signals, this chart shows the L-band
  - Signal plans evolve over time
    - Uncertain if the GLONASS CDMA plans are still accurate
    - Most of these signals are now turned on and ’healthy’
  - ARNS systems constrained to L1 and L5 bands
  - This system covers "everything" in the GNSS L-band



ARFIDAAS 2 - RFI Monitoring System Architecture



ARFIDAAS 3 - RFI Monitoring system unit and data products

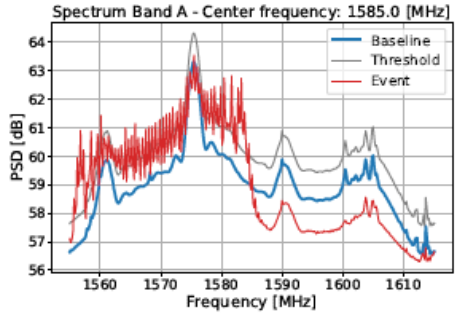
- Results are emailed to stakeholders within 5 minutes
  - Spectral plots and generated reporting help decision making

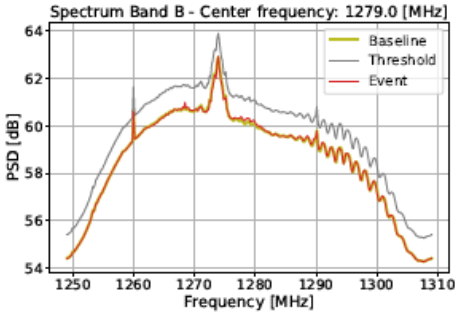
ID: ARFIDAAS_Trondheim_2019_10_31_10_10_29
2019-10-31T10:10:29Z
Input file: Event003.DAT
Dection duration: 3.0 seconds
Analysis window: 1.0 seconds
Bandwidth: 60.0 [MHz]
Monitoring bands' center frequency: A: 1585.0 [MHz]. B: 1279.0 [MHz]. C: 1233.0 [MHz]. D: 1192.0 [MHz].
Antenna type: Novatel_704WB
Location: Norway, Trondheim, site: Trondheim, coordinates: 60N, 11E
Event origin: 0x00000811

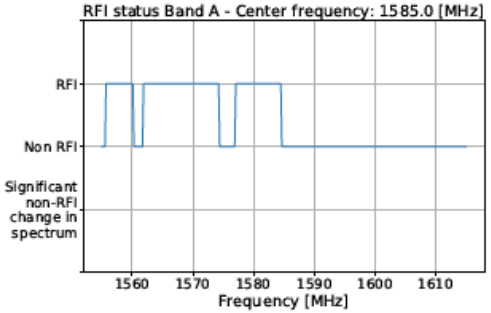
Baseline: RF front end parameters
Avg highband power:-101.81 [dBm] at input
Avg lowband power:-89.47 [dBm] at input
Avg AGC value A: 394.90. Avg AGC value B: 397.70. Avg AGC value C: 393.60. Avg AGC value D: 409.55.

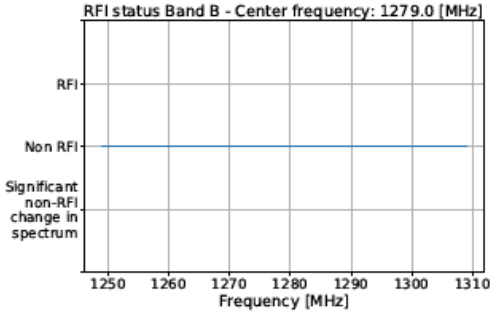
Event003: RF front end parameters
Avg highband power:-93.70 [dBm] at input
Avg lowband power:-89.50 [dBm] at input
Avg AGC value A: 463.09. Avg AGC value B: 397.41. Avg AGC value C: 393.59. Avg AGC value D: 409.57.

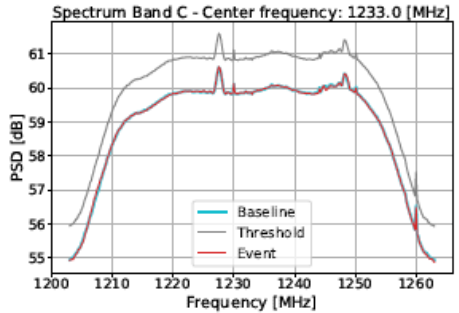
Event003: Frequency analysis
Band A - Center frequency: 1585.0 [MHz]
  Event 1: Event type: WB. Start: 1555.706 [MHz]. End: 1560.294 [MHz]. Max diff: 3.92 [dB]. Mean diff: 1.75 [dB]
  Event 2: Event type: WB. Start: 1561.882 [MHz]. End: 1574.412 [MHz]. Max diff: 2.31 [dB]. Mean diff: 1.11 [dB]
  Event 3: Event type: WB. Start: 1577.059 [MHz]. End: 1584.647 [MHz]. Max diff: 3.49 [dB]. Mean diff: 1.44 [dB]
Band B - Center frequency: 1279.0 [MHz]
  No events detected
Band C - Center frequency: 1233.0 [MHz]
  No events detected
Band D - Center frequency: 1192.0 [MHz]
  No events detected

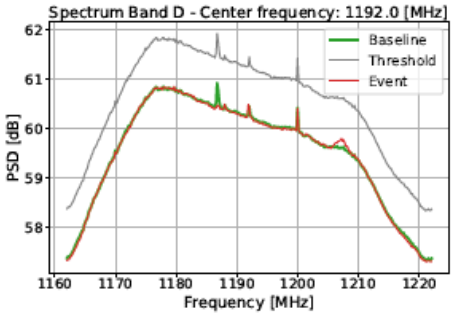












ARFIDAAS 4 – System deployment

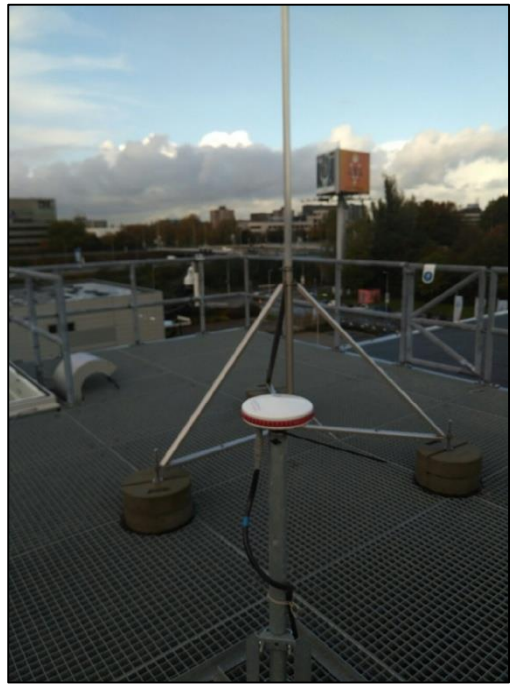
- SINTEF, Trondheim
- SINTEF, Trondheim B
- University of Helsinki
- ESTEC, Noordwijk
- NLR, Amsterdam
- NKOM, Trondheim C
- Indra Navia, Asker
- NKOM, Moss

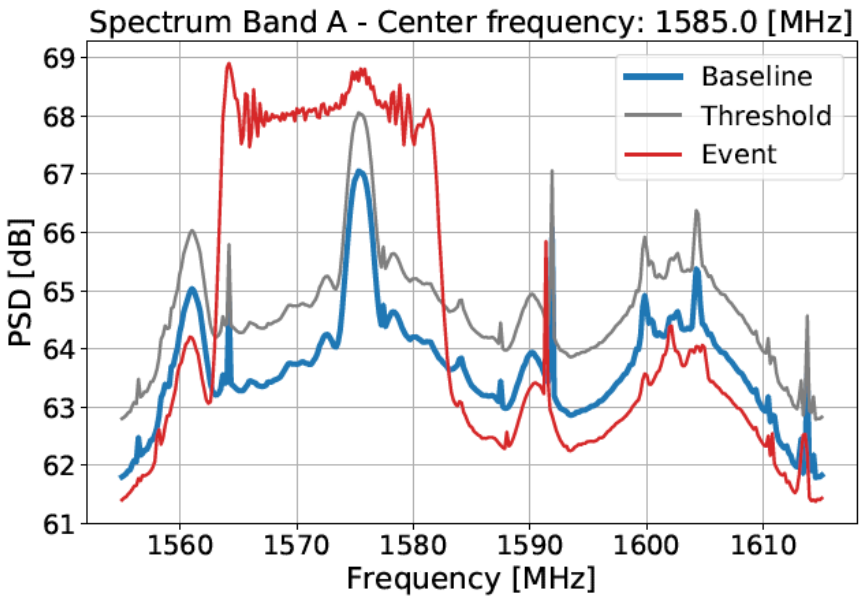
- Pending deployments
  - Czech Republic x2
  - Slovakia x1

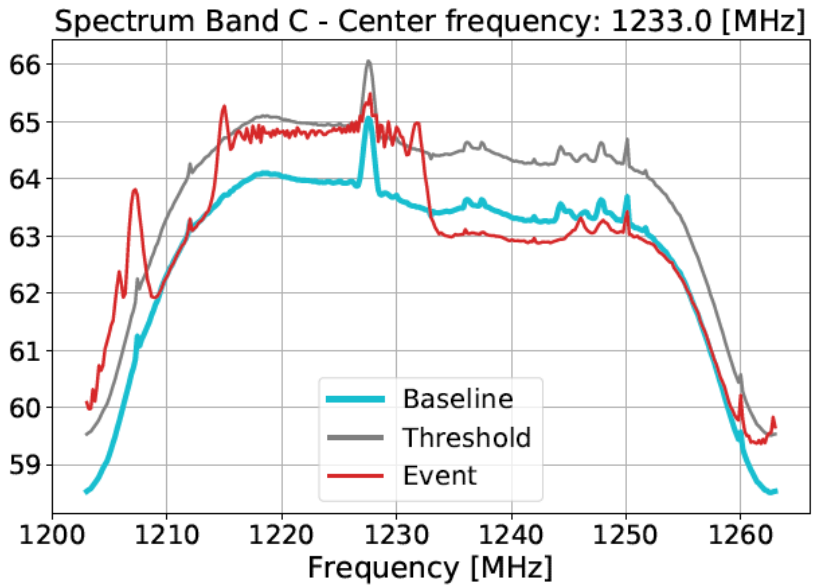
- Map care of creative commons.

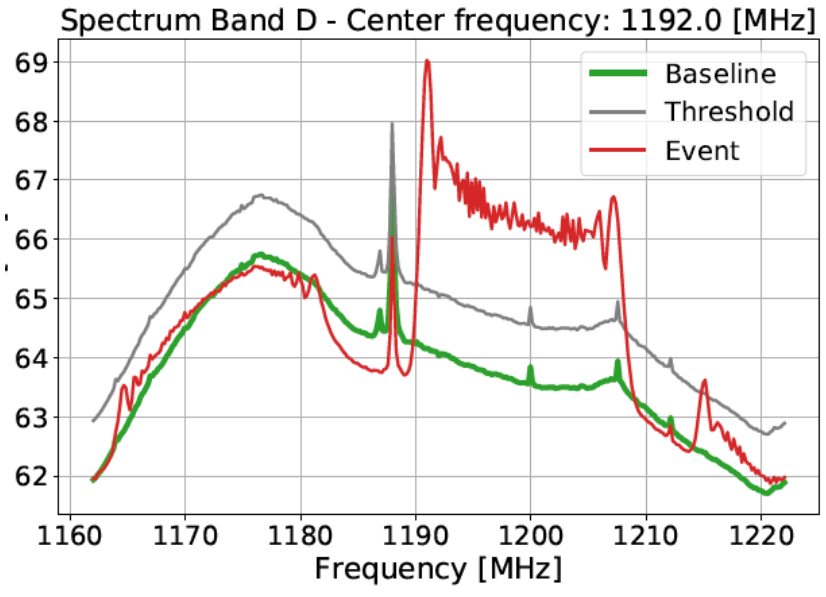
ARFIDAAS – 5

- NLR
- Office located next to a very busy highway
- Known occurrences of RFI based on past investigations
- Instances of triple frequency jamming observed
  - L1+E1, L2, E5B (If we look closely, L5+E5a too?)
  - Just use GLONASS(TM)?









ARFIDAAS 6: The RFI is a problem for high integrity systems

- Observations from 1 to 25 February 2020

Site	Trondheim A	NLR	Trondheim B	Indra	Estec	Helsinki
Number of events	156	139	78	41	3	0
Multi-frequency observed?	no	yes	no	yes	no	n/a

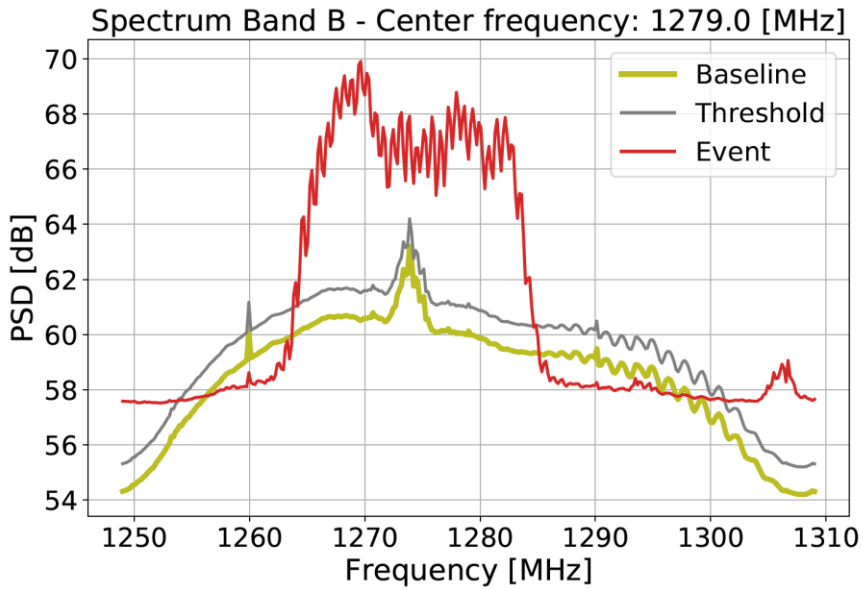
- Helsinki and ESTEC are far removed from busy roadways
  - Trondheim C – not online until April 2020 has over 250 events per month
- For Trondheim A, NLR, Trondheim B, and Indra the average is 4.14 events per day
  - Slightly less than half of these events are thought to be intentionally generated RFI
  - Two events of six seconds per day gives odds of **1.4e-4** of being subjected to intentional jamming at these sites
    - For some systems like GBAS this is already a problem (needs **10^{-7} / 15** seconds approach)
    - Why did we stop on 25 February?

ARFIDAAS 7: E6 is the PRS/HAS(?) signal

- Police and military: Our German+Russian colleages at a recent LATO meeting mentioned issues with their police/military operating jammers and RADAR
  - German police using Jammers up to 20 Watts against drones
  - Russian L1 GBAS from NPPF Spectr jammed by RADAR harmonics
  - Monday 25 Feb. – Fri. 28 Feb.
    - Jamming the entire spectrum between 1240 and 1300+ MHz
    - Periodic every 2+ hours for several minutes
    - Started Monday, Stopped Friday night
    - Visible in Oslo and at both sites in Trondheim though not necessarily simultaneously
  - I believe the target was the RADAR at Gråkalen
    - This alone generated ~100 events at Trondheim prime site

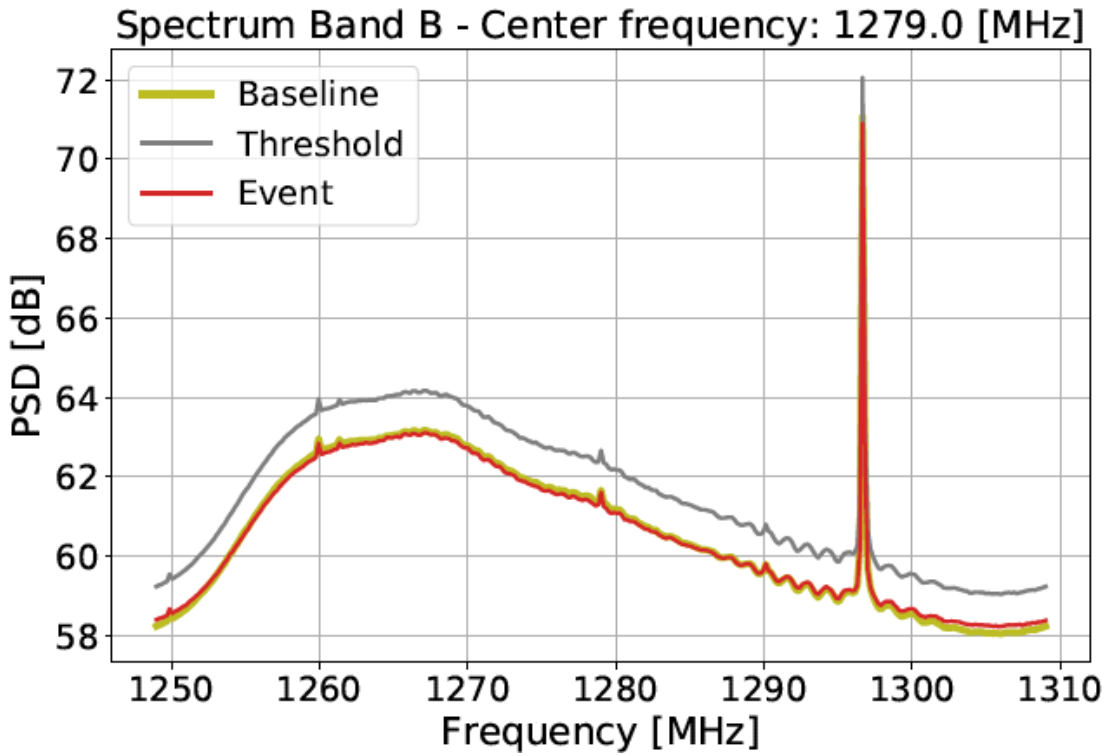
https://www.adressa.no/

Sissel Lynum 24 Feb. 2020



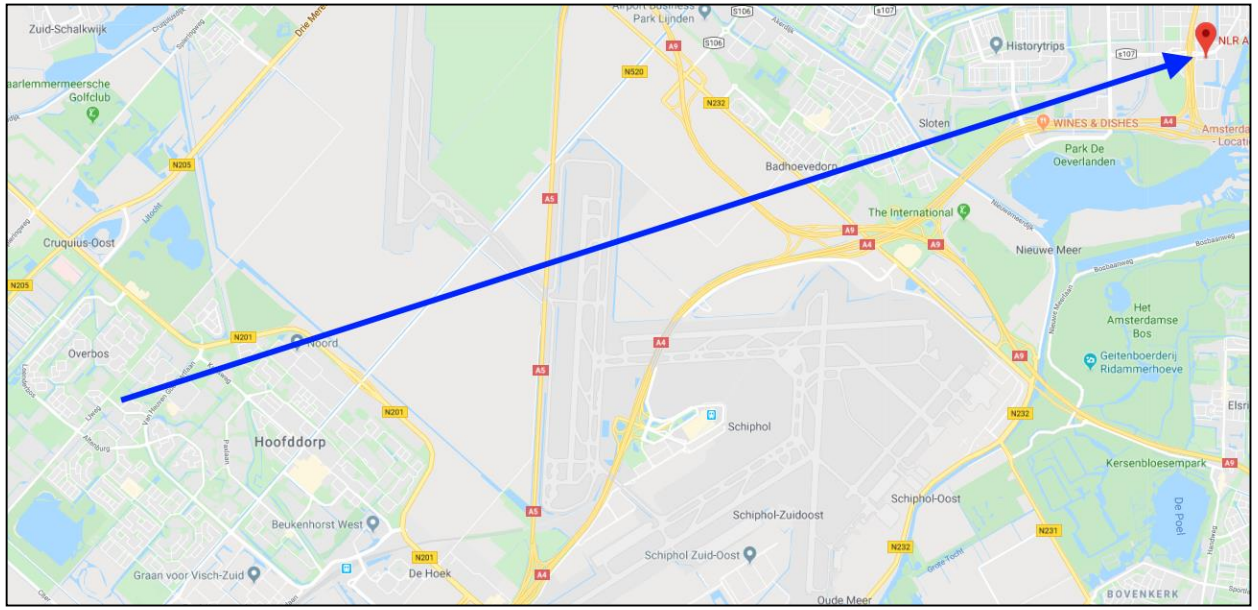
ARFIDAAS 8: All sites have noisy neighbors

- L2 and E6 bands are 'polluted'
- Every single deployment site has observed multiple events affecting only the L2 or E6 bands
  - For four of six sites L2 and or E6 event triggering must be disabled – NLR and ESTEC can see this type of signal
- http://www.pa0ply.nl/1296.htm
- A 300 Watt amplifier through a 28 dB gain dish...



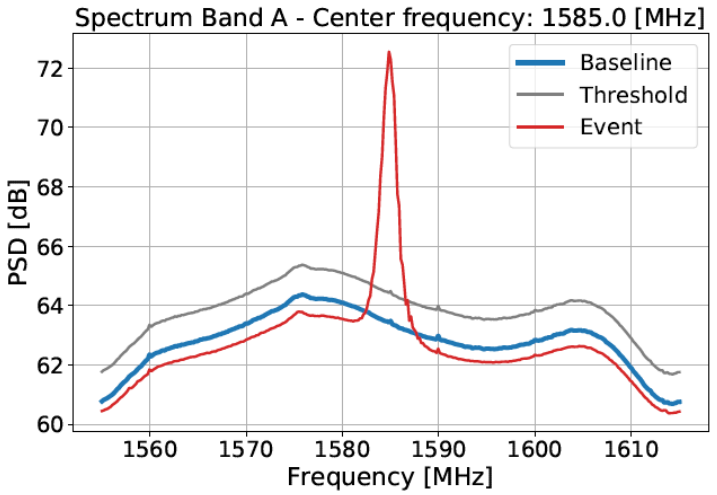
Station outfit:

Transceiver:	TS-2000X
Preamplifier:	VHF Design - 0.3dB
Final amplifier:	300Watt SSPA (DF9IC)
Antenna system:	3m solid dish, Andrews prime focus - 28dBi / Septumfeed modified for f/D 0.32
Control system:	VK5DJ - Stand alone interface

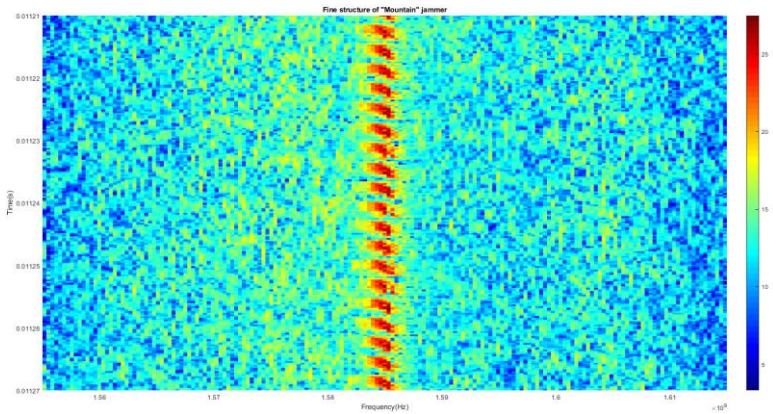


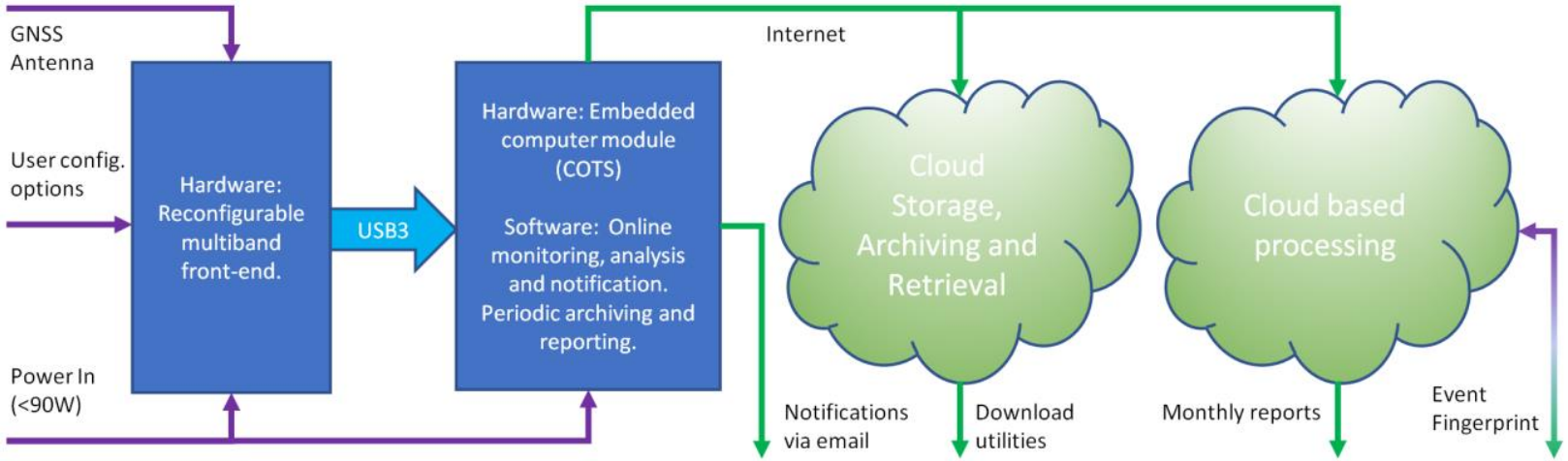
Future Plans 1 – Looking deeper

- Users have indicated that more information is desirable and faster notification
- This helps the decision making process and improves reaction time
  - Important for potentially using the system for enforcement
  - Important for mobile use cases indicated by NKOM



- Example – signal on right initially looks like it's accidental emissions
  - Closer inspection suggests it's maybe a badly made jammer
  - Potential to fingerprint individual jammers



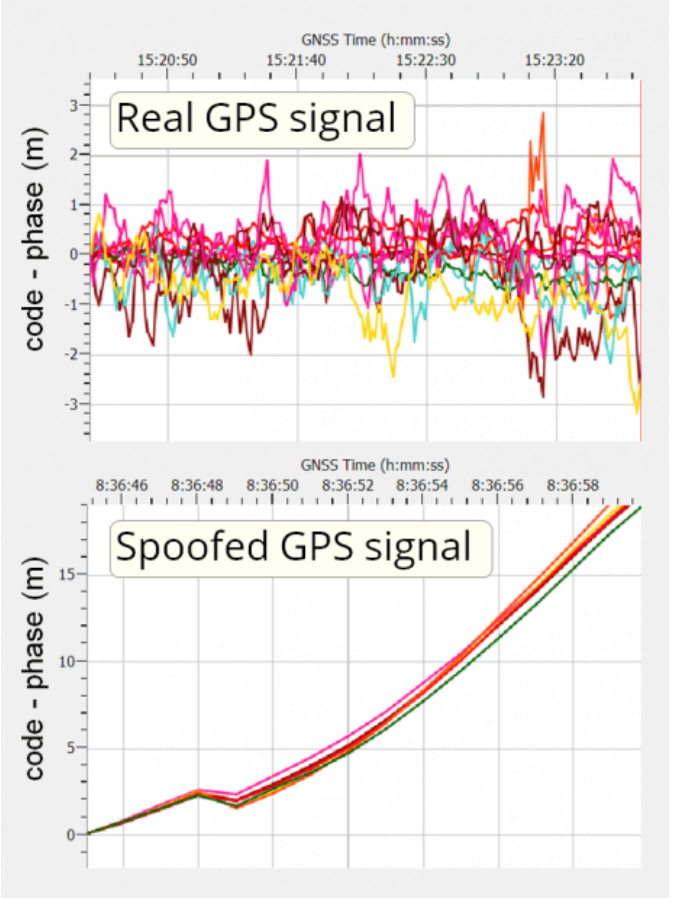


- "Honorable mentions"

SINTEF

Honorable Mentions 1 of 3

- I’ve observed a tendency of manufacturers to make claims about jamming and spoofing
- They aren’t ”””wrong””” (note the triple quotes), but they leave out assumptions
- Example 1 – A high quality GNSS receiver manufaturer in 2017
  - Advertising https://www.septentrio.com/en/insights/spoofing-your-gps-attack-proof
  - Each of the signal parameters they identify as being signatures are spoofable
  - For example – the code-carrier divergence plot
    - This is *not* a fundamental feature of a spoofed signal
    - This is a feature of an improperly configured fractional-N PLL used to spoof a GNSS signal

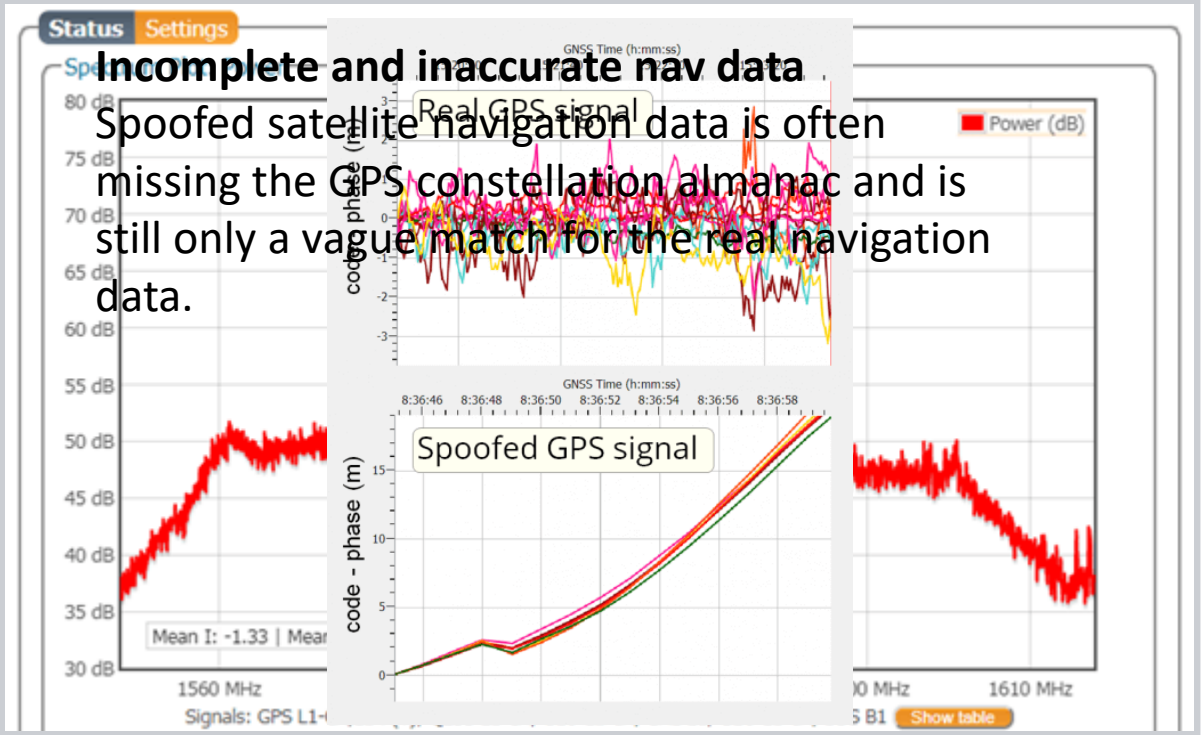


- We decided to prove them wrong because ’why not’
  - https://insidegnss.com/infeasibility-of-multi-frequency-spoofing/
    - Authors, James T. Curran, Aiden Morrison, Cillian O’Driscoll

Honorable Mentions 2 of 3

- We decided to prove them wrong because ’why not’

Claimed by manufacturer	Implemented by three guys in a weekend for fun



Incomplete and inaccurate nav data

Spoofed satellite navigation data is often missing the GPS constellation almanac and is still only a vague match for the real navigation data.

I have a cellphone in my pocket?

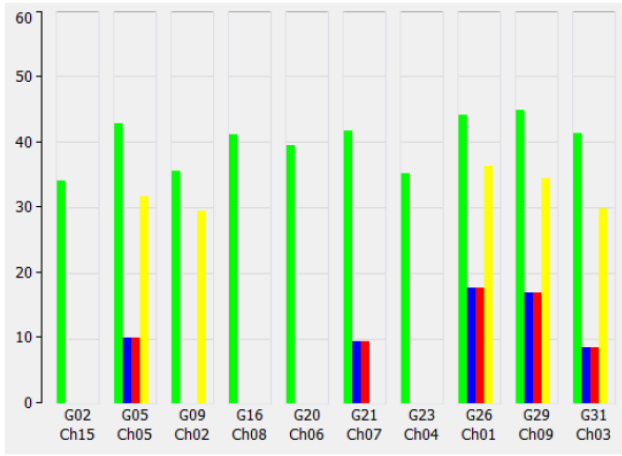


Figure 1: Example of the reported carrier-to-noise ratio for the receiver under test, when broadcasting L1 C/A (green), L1 P(Y) (blue), L2 P(Y) (red), and L2C (yellow) from a narrow-band single-frequency transmitter centered between L1 and L2.

Figure 6: Measured code-carrier divergence on eight spoofed GPS L1 C/A signals over twenty minutes

SINTEF

Honorable Mentions 3 of 3 - Research around secure signals

- Some constellations will broadcast cryptographic sequences that allow ’validation’ that you are receiving the signal from the correct source
  - Galileo has vulnerabilities due to the structuring of its data message that helps attackers guess many bits in advance
    - Additionally if you guess wrong the Forward Error Correction will often correct it for you – thanks!
  - GPS L1C will use a slightly better approach where the PRN is ’punctured’ by a sequence
    - Searching after the fact will expose whether or not this sequence was present, and validate or invalidate the signal
  - However, both are vulnerable to being ’walked away’ by being jammed first then capturing the receiver on a false signal

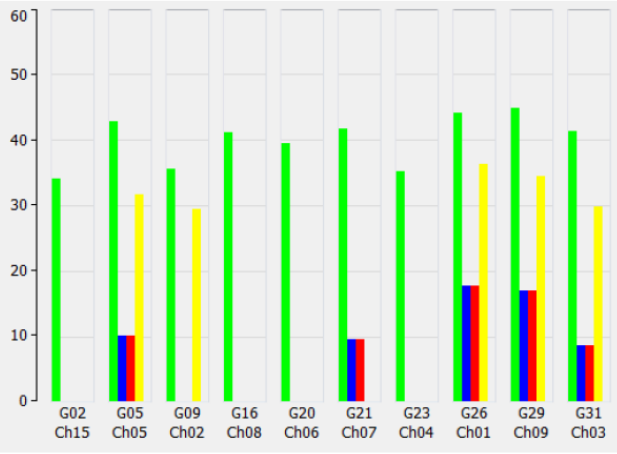


Figure 1: Example of the reported carrier-to-noise ratio for the receiver under test, when broadcasting L1 C/A (green), L1 P(Y) (blue), L2 P(Y) (red), and L2C (yellow) from a narrow-band single-frequency transmitter centered between L1 and L2.

'We hacked U.S. drone': Iran claims it electronically hijacked spy aircraft's GPS and tricked aircraft into landing on its soil

By: Craig Mackenzie and Mark Duell
Updated: 10:36 EDT, 19 December 2011

SINTEF

Conclusions

- 1) RFI is very real
- 2) Once there's an economic motivation for someone to spoof GNSS, they will
  - I see **you** ordered a nice stereo from amazon → I see **I** ordered a nice stereo from amazon.
- 3) It's wishful thinking that there are simple fixes
  - You have to make sure that your system security level makes the attack just not worth it
- 4) You must be very careful when interpreting claims from manufacturers
  - They are probably not lying to you, but they are absolutely not including all the disclaimers

SINTEF

Teknologi for et bedre samfunn