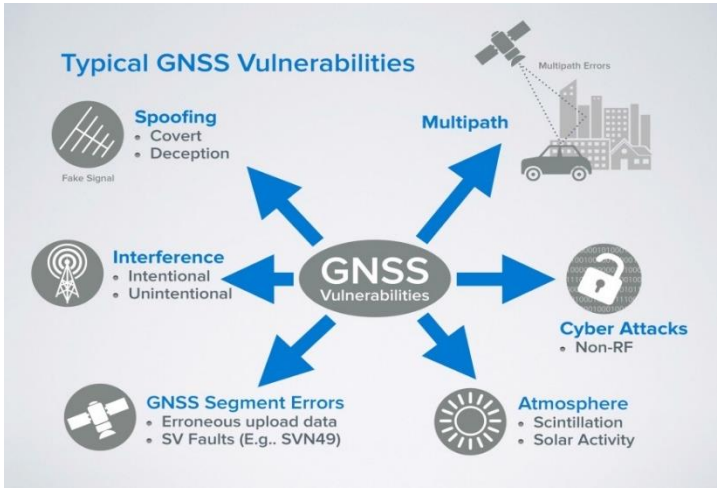
SPIRENT

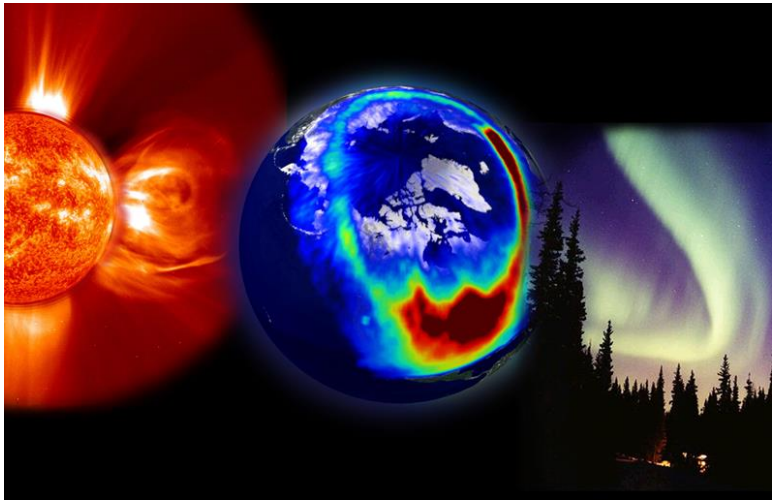
Towards the development of a standard test methodology for measuring the resilience of GNSS devices to real world threats

Guy Buesnel, April 2017

Real world threats to GNSS

Impacting Time and Position



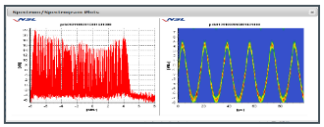


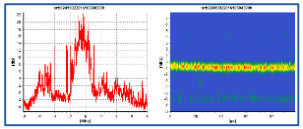
Spirent Paignton, UK

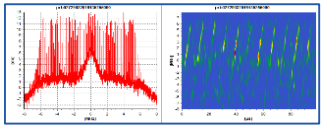
German Airport

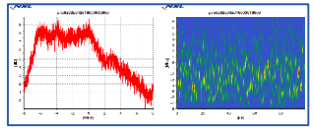
Spirent San Jose, US

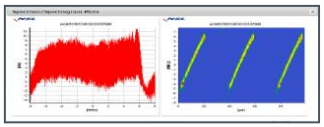
JAPAN

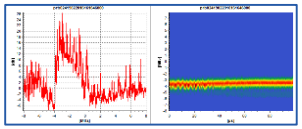


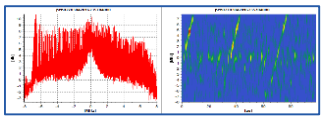


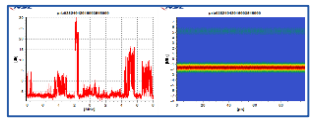


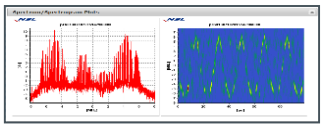


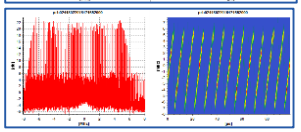


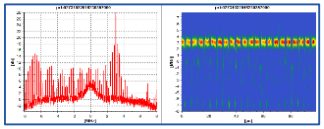


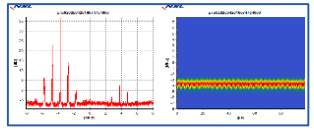












The spread of jamming

Commercial Aviation

- Over 70 incidents of GPS jamming reported by pilots through NASA's Aviation Safety Reporting System (ASRS) since 2013
- Philadelphia North East Airport (PNE) – FCC Agents detected a GPS jammer that was operating in a nearby car park – and requested it to be shut off. Owner subsequently destroyed it
- Marseille Airport (LFML) 2016 – RNAV approaches to RWY 31L/13R and 31R/13L withdrawn due to GPS interference making them unusable
- Manila Airport (NAIA) – Frequent reports of GPS Receiver interference close to Airport by arriving/departing aircraft

Telecoms

- Complaint from a cell provider in Florida that its cell phone tower sites had been experiencing interference: Forfeiture Order affirms proposed $48,000 forfeiture against a man for using a cell phone signal jammer in his car while commuting to and from work on a Florida highway over a 16-24 month period *(Source COPUOS Scientific and Technical Subcommittee Meeting presentation, Feb 2017)*

The spread of GNSS jamming

Author: PatrickMiles November 27, 2012

Quality: ★★★★★

I like that jammer because it is simple. You don't have to be a rocket scientist if you want to use it. Nothing special is here, just plug it in and it is done. Another thing I like about this small gadget is that it has precisely calculated output signal power so it never comes out of my car and that is just perfect because nobody can spot and track that jammer.

Author: AndyDecker November 7, 2012

Quality: ★★★★★

I'm a truck driver and I'm working with one company for almost four years and we've trusted each other. I hauled their cargo and everything was ok, until they have decided to install a tracker in my lorry. I was really angry and I've decided to protect my privacy myself. Now I just plug that thing in my car lighter slot and enjoy my ride!

Author: Stewie October 2, 2012

Quality: ★★★★★

I'm using this GPS jammer for almost a month. I like it, it jams GPS and leaves everything else untouched, exactly what I needed. With it I'm sure I won't be tracked, and it fits my budget!

Drines jamming system

Total RF output power : **550W** (Adjustable output power for each band)
Quadcopters/Drones remote controls frequency taype 6 bands:

1. 5.8Ghz 5500-5900MHz (or 5.0-5.9Ghz) -50W
2. 2.4Ghz 2400-2500 MHz – 100W
3. Remote Control 433 MHz -100W
4. Remote Control 868 Mhz – 100W
5. GPS L2 1227.60 MHz – 100W

Drines jamming system Range: 1500~3000 meters(-75dBm@Omnidirectional antennas).
The jamming distance will be varied depending on the signal strength and location.
Power supply: AC adapter (AC220V-DC27V or 24V/ 40-50 Amp)
Adjustable Output Power each Band, Stand-alone modular design and individual power control.
Temperature over protection.

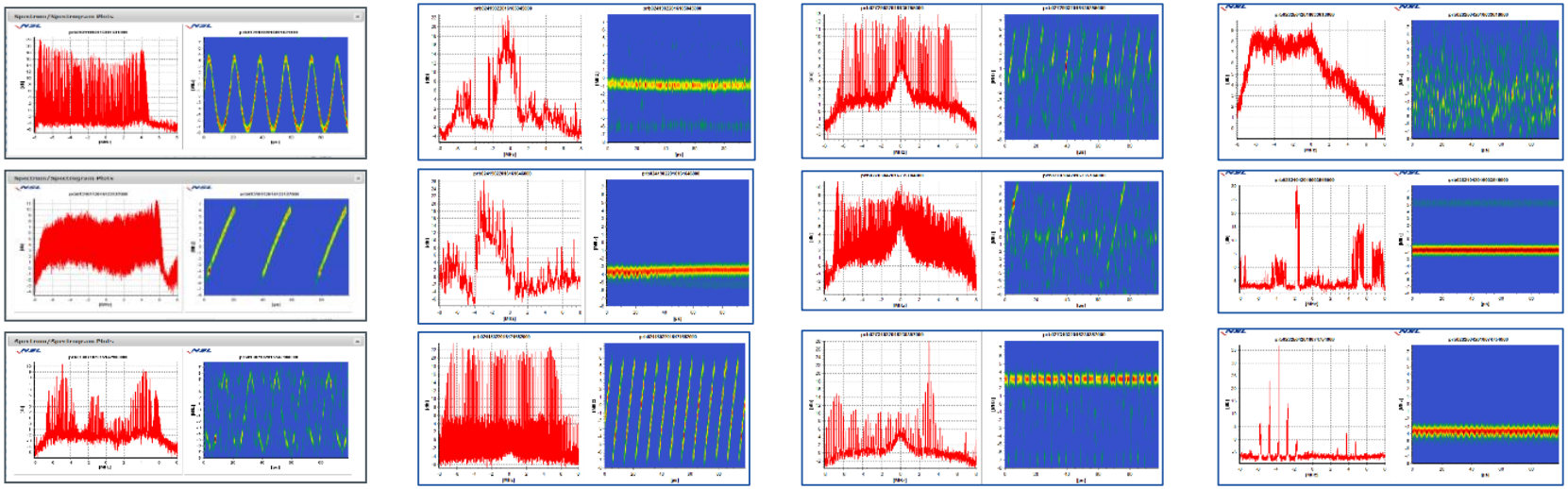
The spread of GNSS jamming

Spirent Paignton, UK

German Airport

Spirent San Jose, US

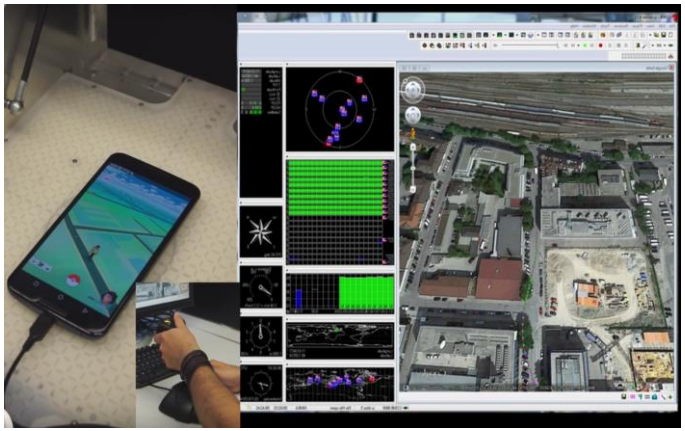
JAPAN

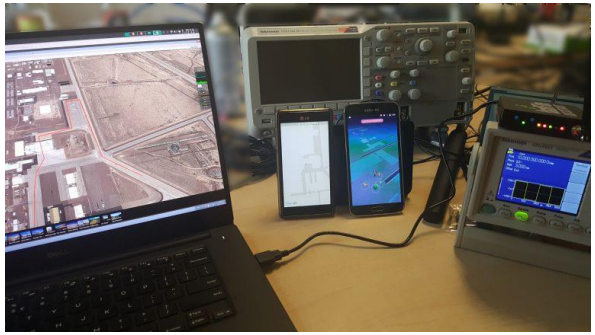


Spirent has captured over 15000 GPS L1 interference events since fielding sensors in 2015 – The GPS L1 spectrum is not clean

Real examples of GPS Spoofing

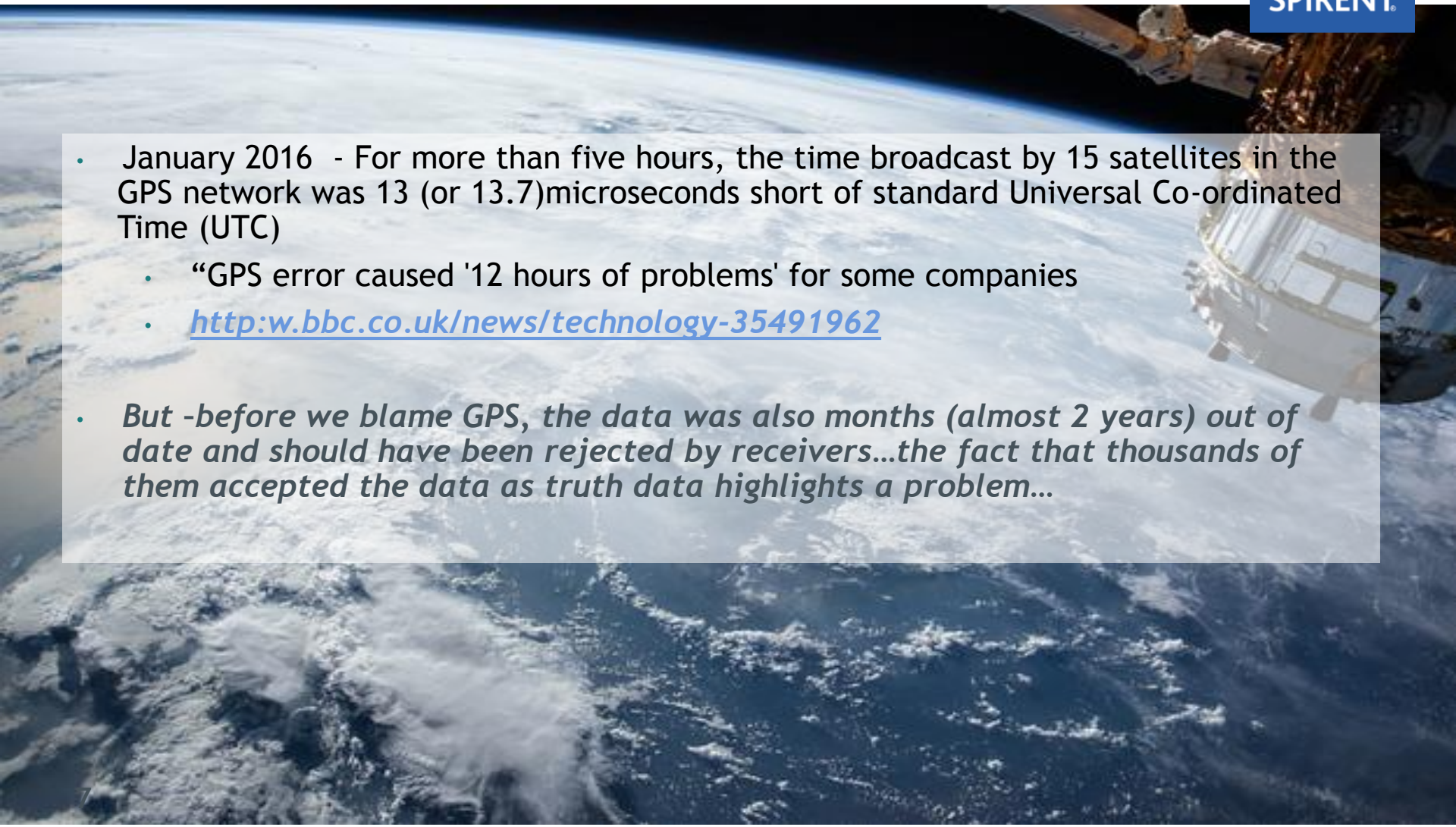
Pokémon GO





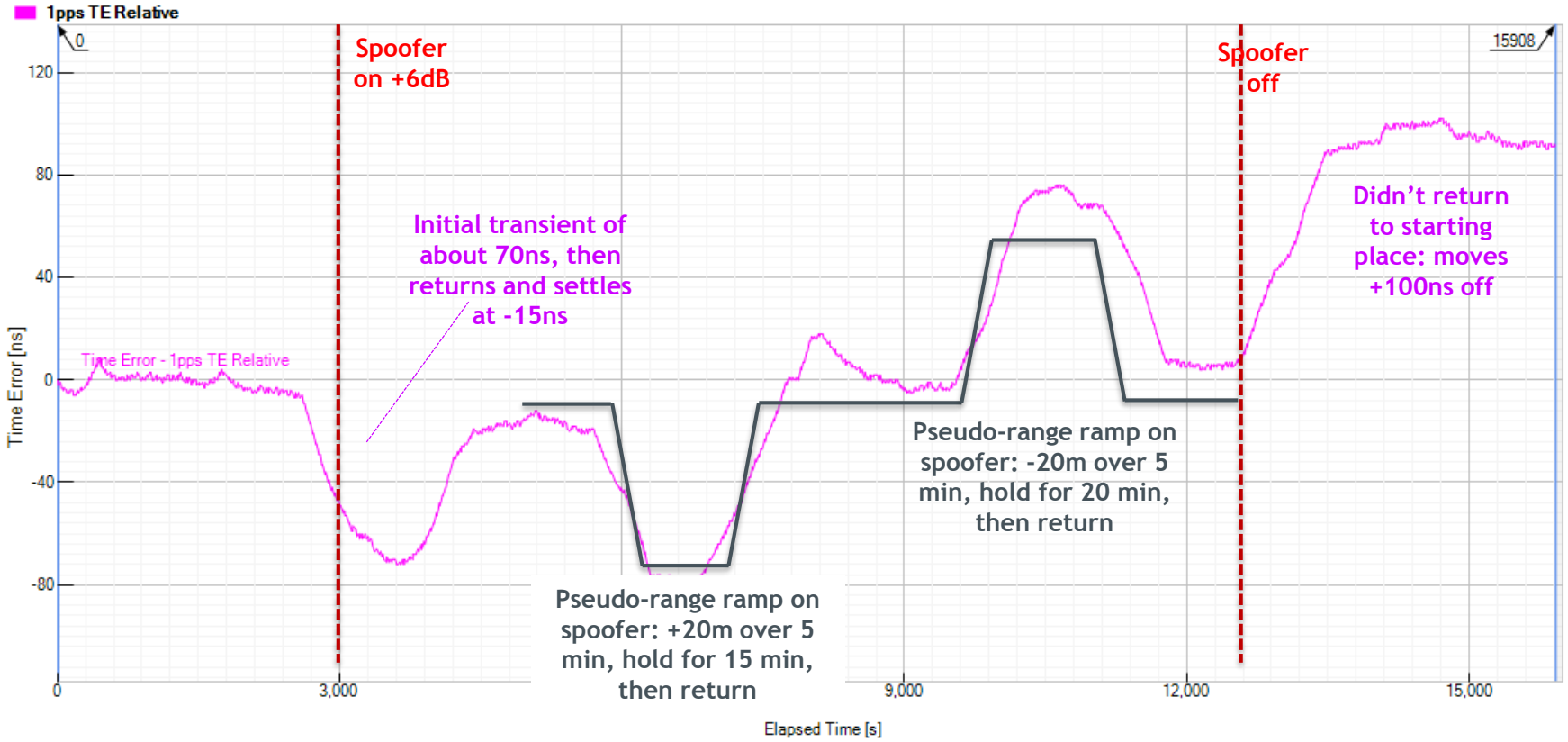
From primitive to sophisticated - GPS hacking in six weeks…

GNSS Segment Errors



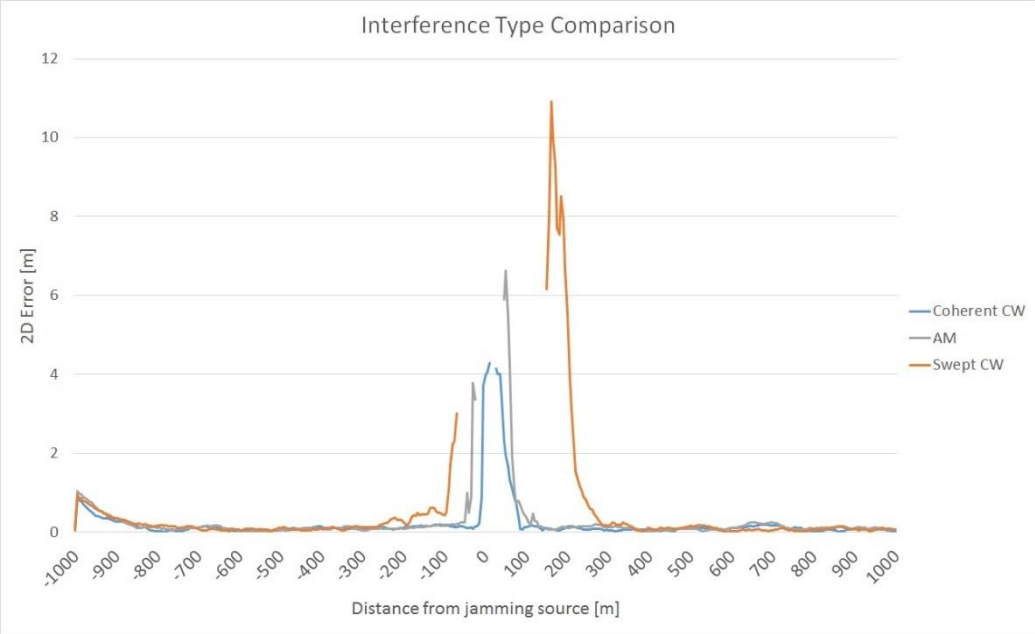
- January 2016 - For more than five hours, the time broadcast by 15 satellites in the GPS network was 13 (or 13.7)microseconds short of standard Universal Co-ordinated Time (UTC)
  - “GPS error caused '12 hours of problems' for some companies
  - *http:w.bbc.co.uk/news/technology-35491962*
- ***But -before we blame GPS, the data was also months (almost 2 years) out of date and should have been rejected by receivers…the fact that thousands of them accepted the data as truth data highlights a problem…***

Why we need to understand resilience

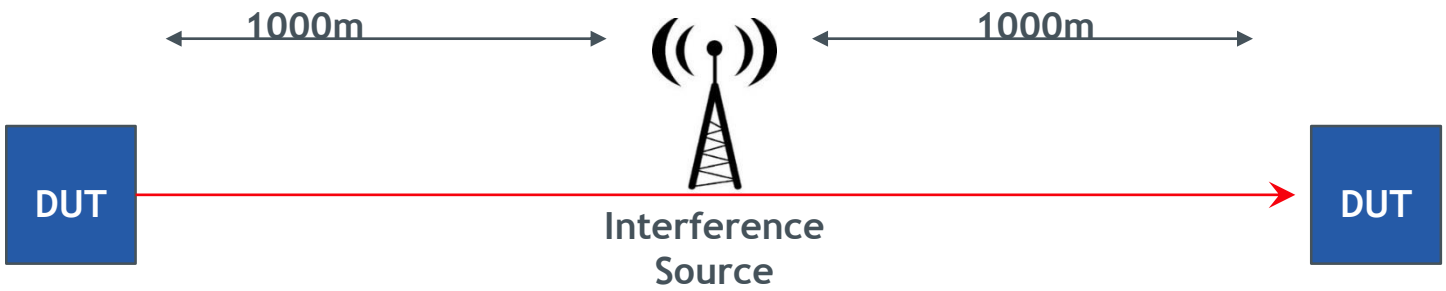


- Timing receiver subjected to introduction of Spoofed GPS signals…

Why we need to understand resilience



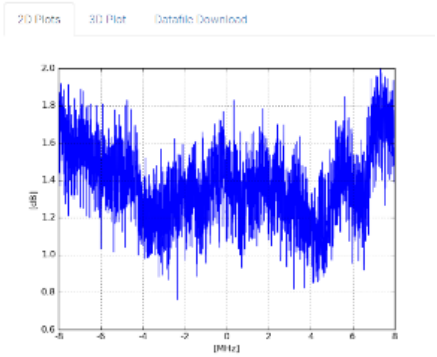
- Receiver A tested against three different interference types
- Note marked differences in receiver behaviour observed against each type of interference



Evaluating Resilience – top level approach

Risk Assessment

Characterisation of environment – derive requirements for operation in degraded/denied GNSS



Test vs threats

Real world threat test of systems and devices

Implement mitigation strategy

Evaluate performance – repeat risk assessment periodically

Specifying resilience levels – through mandatory standards

- European Commission Radio Equipment Directive
  - European CE marking (and testing) for GNSS receivers:
  - Today: Nothing!
  - June 13th 2017: must comply with the “GNSS RED”
- As of this date, GNSS receivers sold in the EU must (legal requirement!) comply with the relevant “RED”…..
- First example of resilience being specified in a standard
  - Adjacent Band Selectivity:
  - Wanted signal(s): GNSS(s) supported by the receiver, applied at nominal level(s) (~-130 dBm)
  - Adjacent band signal (ABS) (interferer) : 1MHz wide, filtered AWGN signal
  - Performance metric: C/N0 as reported by the receiver in tracking mode
  - Requirement: <1 dB degradation of C/N0 when ABS is added at five frequency offsets and levels

Why should I care?

- Must test each GNSS supported by the device (GPS, Galileo, GLONASS, Beidou, SBAS, if supported) for any degradation in C/N0 when an “interfering” signal is applied

- What products will be covered?
  - Any and every product with a GNSS receiver - scientific, commercial, consumer (but not for aviation, maritime, military or government), including timing receivers and products
    - Sports watches, mobile phones, “sat-navs”, agricultural equipment, surveying equipment, timing equipment, drones etc. etc....

- Who will do the testing?
  - The product manufacturer is responsible for the testing
    - “In-house” or third-party test lab or …..

How good is the metric?

- Top level objective – to show that equipment does not suffer any degradation in performance from Adjacent band noise
- For timing receivers, CN0 not very good at measuring stability..
- Consideration: a universal measurement that covers degradation in performance – otherwise GNSS equipment in every application area would employ a different metric… the most suitable for their area
- CN0 used by DoT in ABC tests in USA – and can be applied to all GNSS devices
  - CN0 the “best metric” for application across all GNSS devices

Other Standards…

- ETSI TS 103 246-3 V2.0.7 (2016-10)
- Satellite Earth Stations and Systems (SES);
  GNSS based location systems;
  Part 3: Performance requirements
- [Release 2.0.7]
- No plans to mandate this standard but could be used in procurement or recommended by regulators

5.4 GNSS Time Accuracy

5.4.1 Definition

GNSS Time Accuracy is the difference between the true GNSS time (reference time of the GNSS system) and the time computed by the GBLS System.

For example, applications requiring synchronization of assets distributed across wide geographical areas can use GNSS time as a reference.

5.4.2.2 Use case: Static Location Target

5.4.2.2.1 Operational environment: Open area

The performance requirements are specified in table 18.

Table 18: Performance requirements for GNSS Time Accuracy, Static location target, Open area

Metric	Maximum time error (ns)		
	Class A	Class B	Class C
Mean value	**6**	**17**	**70**
95th percentile	**17**	**50**	**117**

5.4.2.2.2 Operational environment: Urban area

The performance requirements are specified in table 19.

Table 19: Performance requirements for GNSS Time Accuracy, Static location target, Urban area

Metric	Maximum time error (ns)		
	Class A	Class B	Class C
Mean value	**216**	**260**	**520**
95th percentile	**440**	**483**	**927**

5.4.2.2.3 Operational environment: Asymmetric area

The performance requirements are specified in table 20.

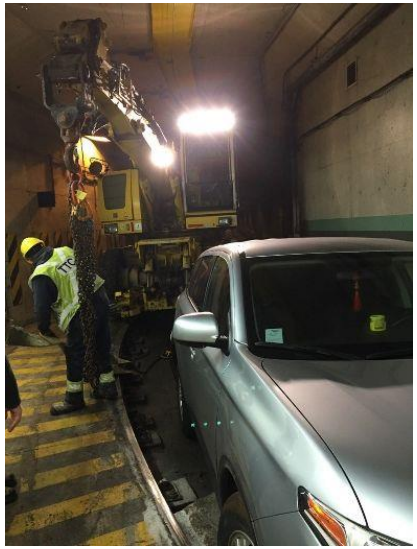
Table 20: Performance requirements for GNSS Time Accuracy, Static location target, Asymmetric area

Metric	Maximum time error (ns)		
	Class A	Class B	Class C
Mean value	**403**	**517**	**670**
95th percentile	**653**	**850**	**1 557**

Note the classification of performance – Classes A, B, C – intent to be able to select a GNSS device for a particular application by "picking" a class in each performance category

Spirent Insights

- GPS / GNSS has unique advantages and will remain as a key component for Position, Navigation and Timing for the foreseeable future
- Interference threats are widespread – the GNSS spectrum isn't clean
- Other threats are also important to consider – e.g, Solar Weather, Scintillation, Spoofing, Segment errors.
- Our evidence shows that real world GNSS threats are adversely affecting PNT systems in unexpected ways
- Important not to be left in the dark – Spirent recommend a proactive approach to ensuring robustness/resilience in GNSS systems
- GPS/GNSS does need to be used within a PTA framework – Good systems engineering practice is to use a complementary PNT system, such as e-LORAN (for timing, essential to have independent route to UTC traceability)



The GNSS Over-Reliance Club

guy.buesnel@spirent.com

http://www.spirent.com/Solutions/Robust-PNT

Join the GNSS Vulnerabilities group on LinkedIn to find out more about GNSS jamming and spoofing