Resilient PNT Resource Guide 2019

Guy Buesnel, CPhys, MInstP, FRIN
PNT Security Technologist, Spirent
May 2019

US Coastguard Problem Reports

Problem Reporting website now online….

- **Plovdiv, Bulgaria, May 2019:** *"From August last year the clock in almost all [vehicle type] with original navigation are showing wrong date, the year is 1999 the daylight saving time is incorrect due to months mismatch, but the time is correct just 1 hour backward, it now shows November 1999 or something. This problem is massive a lot of people are complaining. Please tell me what happened from August last year so old receivers decode date and year wrong, but newer are alright."* (editors note: this is a Week Number Roll Over issue)

- **Port Said, April 2019:** *"User: [Vessel] was effected by the repetitive loss of GPS signal, affecting radar, ais, and gyro input. [Vessel] location was the Port Said EGYPT anchorage. This occurred from 1800 24 April, thru 0330 25 April, while my ship and numerous other ships were attempting to transit the Suez Canal."*

- **Raleigh-Durham, US, November 2018: "***GPS unit has ceased to display valid date and time information and reverted to the year 1999. I contacted the manufacturer who denied any manufacturing defects and could not offer a solution except to obtain another device at my expense (out of warranty for several years). Date/time of problem onset is estimated."* (editors note: this is a Week Number Roll Over issue)

- **Jeddah, Saudi Arabia, October 2018:** *"Before Departure from port of Jeddah Saudi Arabia in Red Sea both GPS were found out of order. There seemed to be GPS signal interference resulting in loss of signal, missing COG / SOG and absence of GPS signals affecting bridge navigation and other communication equipment. GPS screen showing no available satellites in the vicinity, no Lat/Long could be obtained. GPSs restarted - no effect. Pilot advised that tugs reported absence of GPS signal as well. After vessel was cast off situation remained unchanged so own position was obtained by visual and radar observations and frequently plotted in ECDIS as manual fix position. ECDIS was turned to Dead Reckoning mode. Approximately 10 nm away from port area both GPS recovered the signal. After calling few nearby vessels by VHF found out that GPS signal loss problem was common in this area. Also experienced that on private smartphones (verified by Master and 2/Off) it was impossible to obtain GPS position, the signal was not available"*

https://www.navcen.uscg.gov/?Do=GPSReportStatus

Conference/seminar highlights 2019

2019 Highlights

Dates	Conference	Venue	Country	Website
04-06 June	TU Automotive	Suburban Collection Showplace Detroit	USA	https://automotive.knect365.com/tu-auto-detroit/
25-27 June	Autonomous Ship Symposium	Amsterdam RAI	NL	www.autonomousshipsymposium.com
9-11 July	UK Space Conference	ICC near Newport	Wales	https://www.ukspace2019.co.uk/ehome/index.php?eventid=200183909&
15-18 July	Automated Vehicle Symposium	Orlando World Centre Marriott	USA	http://www.auvsi.org/autonomous-vehicles-symposium-moves-orlando-2019
08-11 Aug	DEFCON 27	Paris/Ballys, Las Vegas	USA	https://www.defcon.org/
14-16 Aug	USENIX Security Symposium	Hyatt Regency Santa Clara	USA	https://www.usenix.org/conference/usenixsecurity19
10-13 Sep	DSEI (Defence and Security Equipment International)	Excel Centre	London	https://www.dsei.co.uk/welcome-to-dsei-2019#/
16-21 Sep	ION GNSS+	Hyatt Regency, Miami	USA	https://www.ion.org/gnss/index.cfm
16-17 Sep	Cognizant Autonomous Systems for Safety Critical Applications	Hyatt Regency, Miami	USA	https://www.ion.org/cassca/
21-25 Oct	ITS World congress	Suntec Singapore	Singapore	https://itsworldcongress2019.com/
04-07 Nov	ITSF (Global Conference on Timing and Synchronisation Across Networks)	Hilton Brighton Metropole	UK	http://itsf2019.executiveindustryevents.com/Event/#programme
18-21 Nov	Royal Institute of Navigation International Navigation Conference (INC)	Edinburgh International Conference Centre	UK	https://rin.org.uk/events/EventDetails.aspx?id=1135239

Useful websites…

US Government GPS public portal

https://www.gps.gov/

US Coastguard Navigation Centre

https://www.navcen.uscg.gov/

Resilient Navigation and Timing Foundation

https://rntfnd.org/

Spirent Communications – Robust PNT

https://www.spirent.com/pnt/measuring-resilience

Royal Institute of Navigation – Resilient Navigation Resources

https://rin.org.uk/page/ResilientPNT

Other useful links

- Reliance and vulnerability of Global Navigation Satellite Systems – report by the Royal Academy of Engineering
  https://www.raeng.org.uk/publications/reports/global-navigation-space-systems
- The economic impact on the UK of a disruption to Global Navigation Satellite Systems (published 6 June 17)
  https://www.gov.uk/government/publications/the-economic-impact-on-the-uk-of-a-disruption-to-gnss
- Satellite-derived time and position: Blackett review exploring the dependency of the UK on global navigation satellite systems (published 30 Jan 2018)
  https://www.gov.uk/government/publications/satellite-derived-time-and-position-blackett-review
- GPS / global navigation satellite system vulnerabilities: FAQ
  https://www.spirent.com/go/gnss-gps-faqs/vulnerability
- The evolution of global navigation satellite system spoofing – technology evolution / revolution (published December 2018)
  https://www.gps.gov/governance/advisory/meetings/2018-12/goward.pdf
- How to assess and make business decisions about technology and information risks from the UK National Cyber Security Centre
  https://www.ncsc.gov.uk/guidance/risk-management-and-risk-analysis-practice
- LinkedIn group on GNSS vulnerabilities
  https://www.linkedin.com/groups/8178083/

Detect and Identify

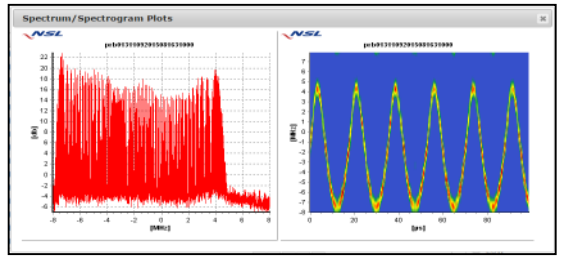
Potential Deployment of Solutions

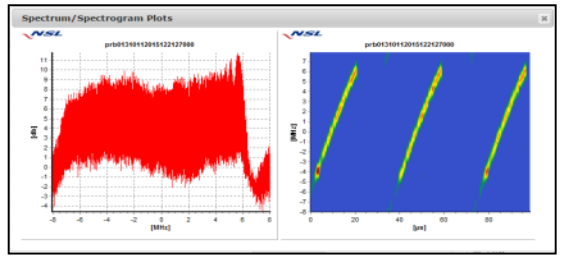
- Fixed Locations
  - Deploy at fixed locations
    - Airports
    - Cities
    - Research Facilities
    - Universities
  - Notification and Storage of any Abnormal signal or disturbance
- Mobile/Field Device
  - Deployed in mobile environments
    - Mobile vehicles
    - People/Soldiers
  - Ability to Capture and Replay

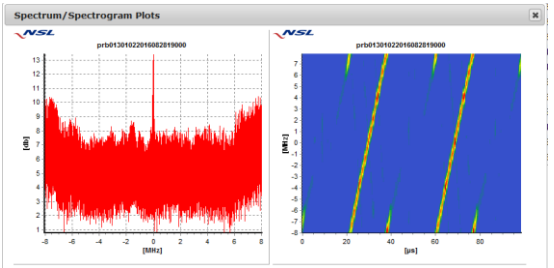
Capture of data

Detector & Data-Server

- Monitor
- Detect
- Notify
- Store





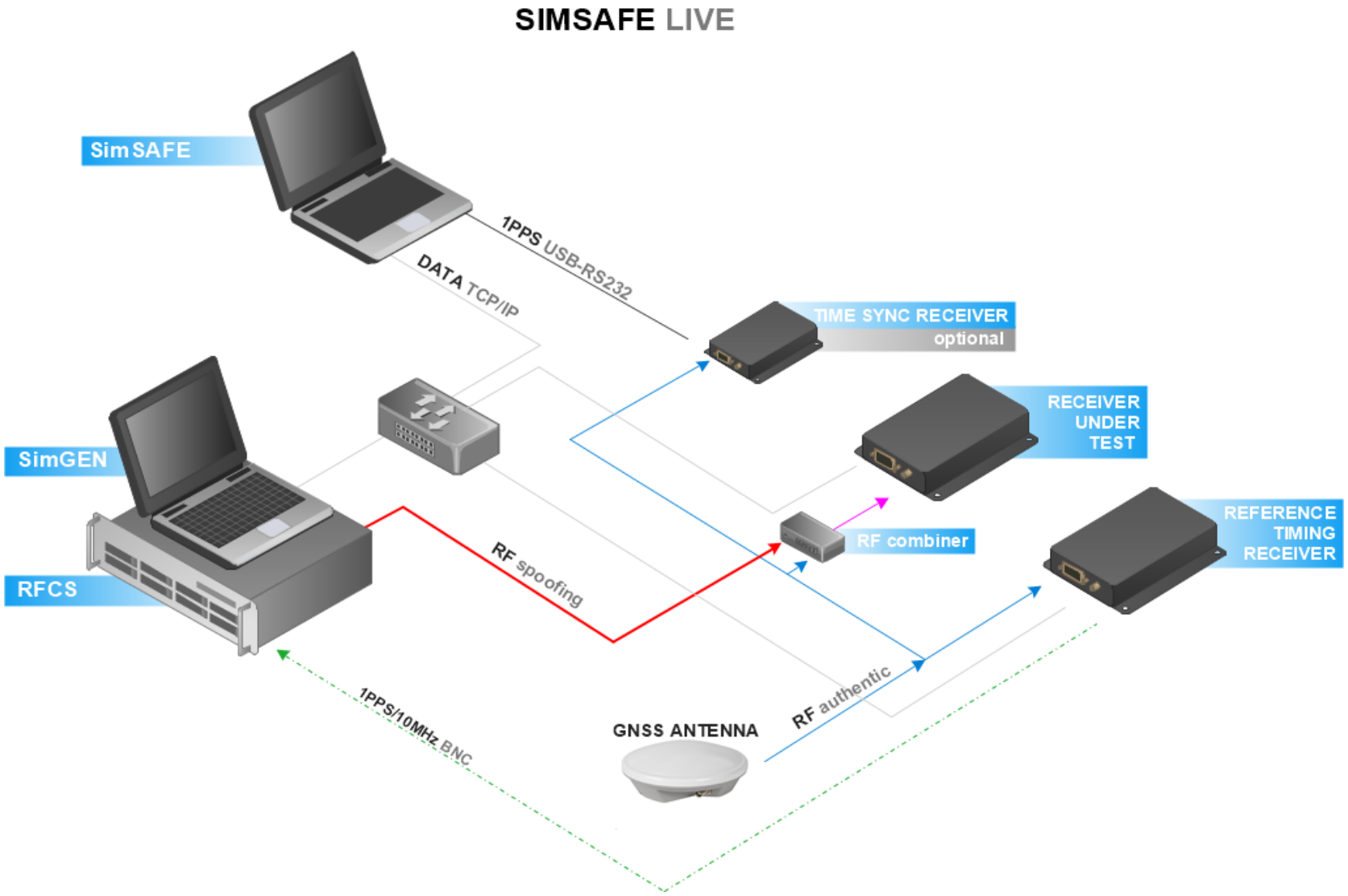


- GPS L1 RFI DETECTORs deployed world-wide since May 2015
- All sites show RFI events that will affect GPS
- “Noisy” sites have hundreds of events per week with several high events every day

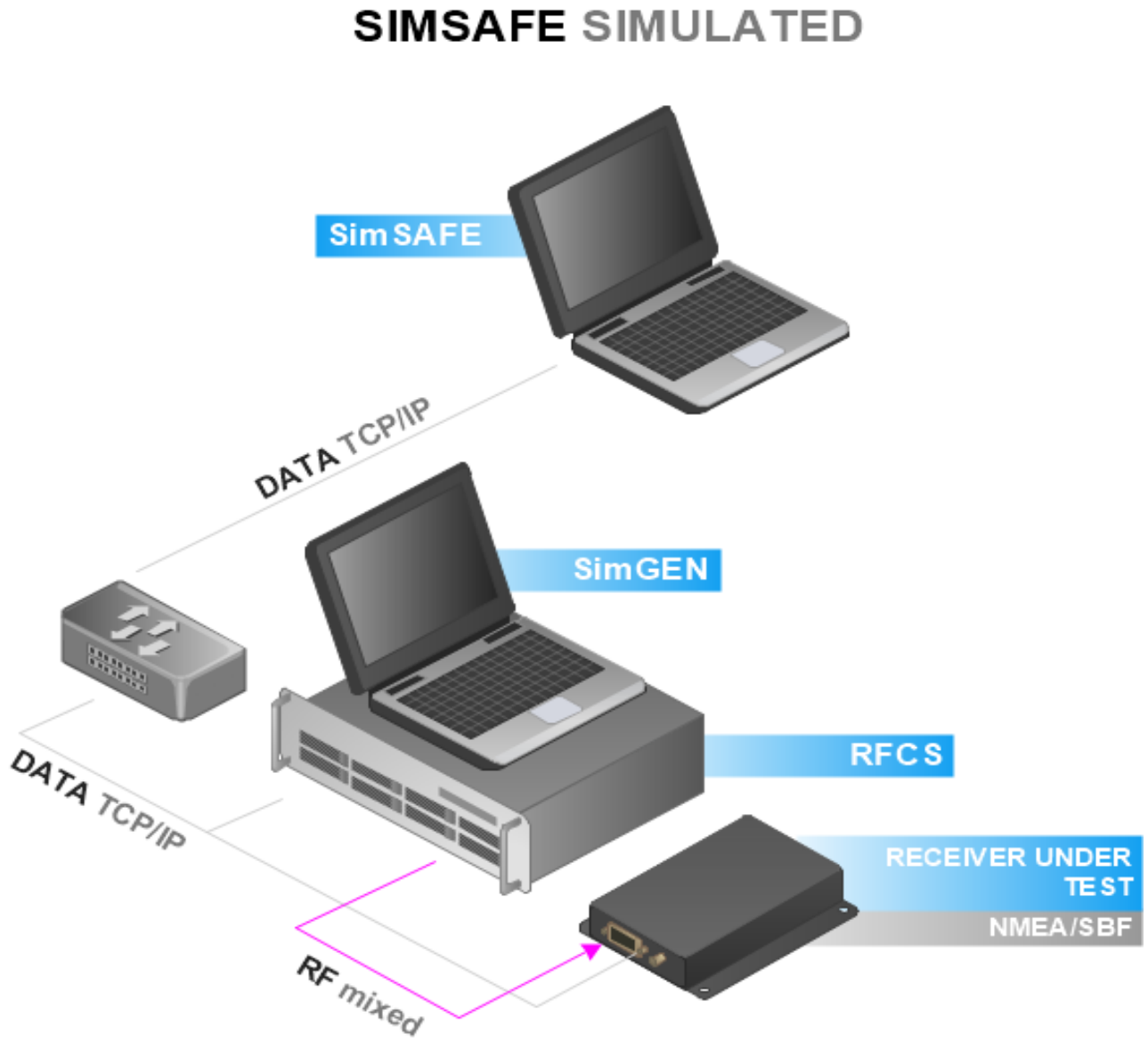
Intelligence through analysis

- Event view:
  - Spectrum
  - Spectrogram
  - Type of interference
  - Priority
  - UTC timestamp and duration
  - Power info
- Analytics for trend analysis
- Jammer “fingerprinting”
  - Most jammers have unique signatures

Spirent Spoofing test-bed



Spirent Spoofing test-bed



Spirent Spoofing Test-bed

Multi/Single channel (loosely synchronized) with smooth deception signal

- The attacker creates one or more deception signals starting with an initial offset between 500 to 600 metres and an attenuation of 10 dB.
- A pseudorange ramp decreases the code delay (you must take into account the bandwidth of the receiver PLL when you determine the pseudorange ramp speed that results in a Doppler offset). When the code delay (relative to the true signal) is close to zero, increase the strength of the deception signal to force the receiver correlator to lock on to the new, false, signal.
-

Multi/Single channel (loosely synchronized) with fixed Doppler offset

- This attack is the same as before, but the deception signal does not change its Doppler. The code/carrier delay (with respect to the Line of Sight) changes in steps of 5 to 10 metres, or uses a pseudorange ramp.

Trajectory spoofing

- The deception signals are consistent with an attacker defined spoofing trajectory. The relative dynamics between spoofer and victim can be simulated.

Multi/Single channel (tightly synchronized)

- The deception signal is generated with an initial code delay (with respect to the Line of Sight) of few metres. The strength of the deception signal slowly increases, starting with an initial attenuation of 5 to 10 dB. The deception signal then slowly moves away from the Line of Sight, causing a position shift and avoiding the loss of lock.

Sinusoidal deception signal

- The deception signal attempts to attack more than one receiver in a given area by changing the code and signal strength with a sinusoidal pattern.

Jam rather than spoof

- To avoid detection of an attacking signal based on signal strength or tracking function and then forcing the receiver to shift to acquisition state, you can perform a jamming attack before the spoofing attack (for example, signal record and replay, signal simulation and loosely synchronized spoofing) resulting in loss of code lock

Navigation data modification

- The deception signal degrades the position calculated by the receiver by changing the content of the navigation messages used in the position calculation

Data replay attack

- The deception signal is generated by replaying data from space, in order to cheat any detection based on space data authenticity verification

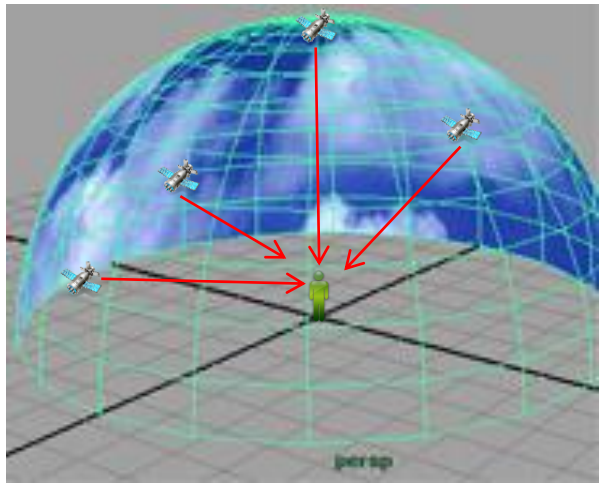
Timing spoofing attack

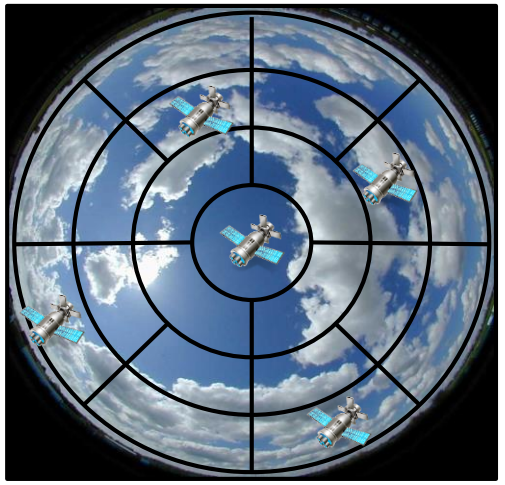
- The attacker creates one or more deception signals with a fixed delay, a constantly increasing delay, or a parabolic increasing delay. The attacker increases the power strength of the deception signals to force the receiver correlator to lock on the new, false signal. The effect is a poisoning of the receiver clock

OTA testing using a Zoned Chamber

Principle of operation – Spirent proprietary system

- The zoned chamber divides the visible sky into a number of '*zones*'
  - Imagine standing at the centre of a dome
- GNSS satellites in the sky will be present in one of the zones



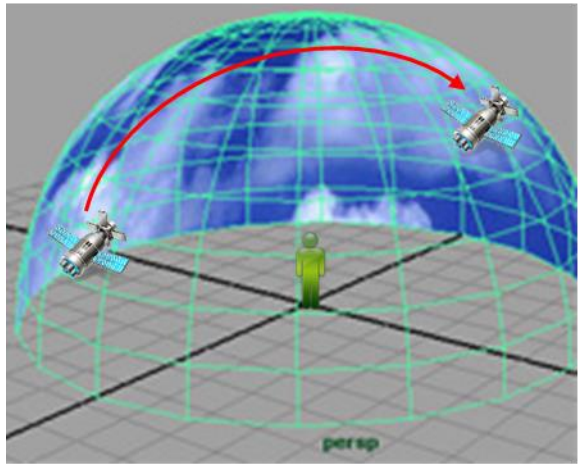


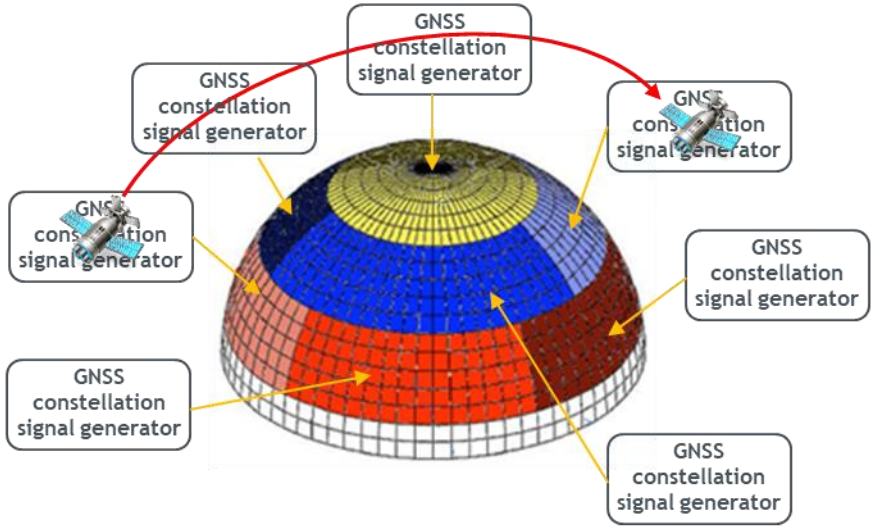
OTA testing using a Zoned Chamber

Supports long scenario and vehicle motion

- The zoned chamber system provides one signal generator RF output per zone
- Each output will simulate the effects of a satellite whilst it is present in the zone
- As the satellite orbit passes across the sky it moves between zones.
  - The simulated signal it ‘handed over’ from one signal generator to the next

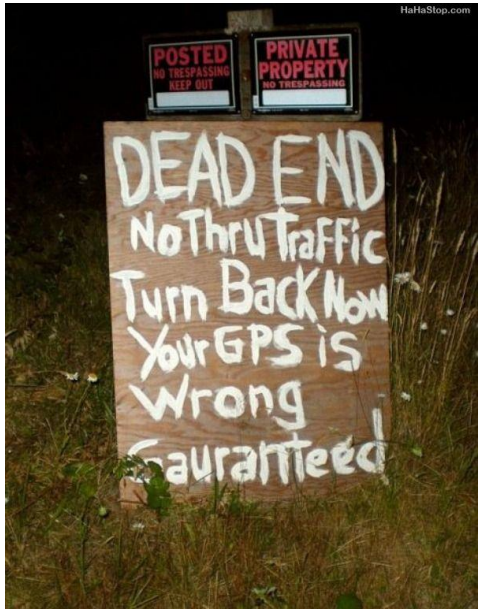
➔ System supports arbitrary time, date, location & motion





Any questions? We can help..

guy.buesnel@spirent.com



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

https://www.linkedin.com/groups/8178083/