spectracom

Time Synchronisation and GNSS Vulnerabilities

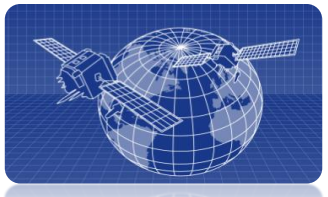
ITSF 2016

Spectracom

- Data centers and financial
- Defense & aerospace
- Communications & global networks
- Emergency services and security
- Digital broadcast
- High end test & measurement
- GNSS simulation







Upcoming Leap Second Event

LEAP SECOND: A one-second adjustment that is occasionally applied to Coordinated Universal Time (UTC) in order to keep its time of day close to the mean solar time, or UT1.

December 31, 2016 @ Midnight UTC

Start testing now！

spectracom

Sources of GNSS Interference

LOSS OF GNSS SIGNAL

- **Example:** Someone accidentally cuts the cable to antenna
- **Impact:** Go into holdover mode, run off internal oscillator

GNSS PERTURBATIONS

- **Example:** Solar events, Ionospheric conditions, etc.
- **Impact:** Go into holdover mode, run off internal oscillator

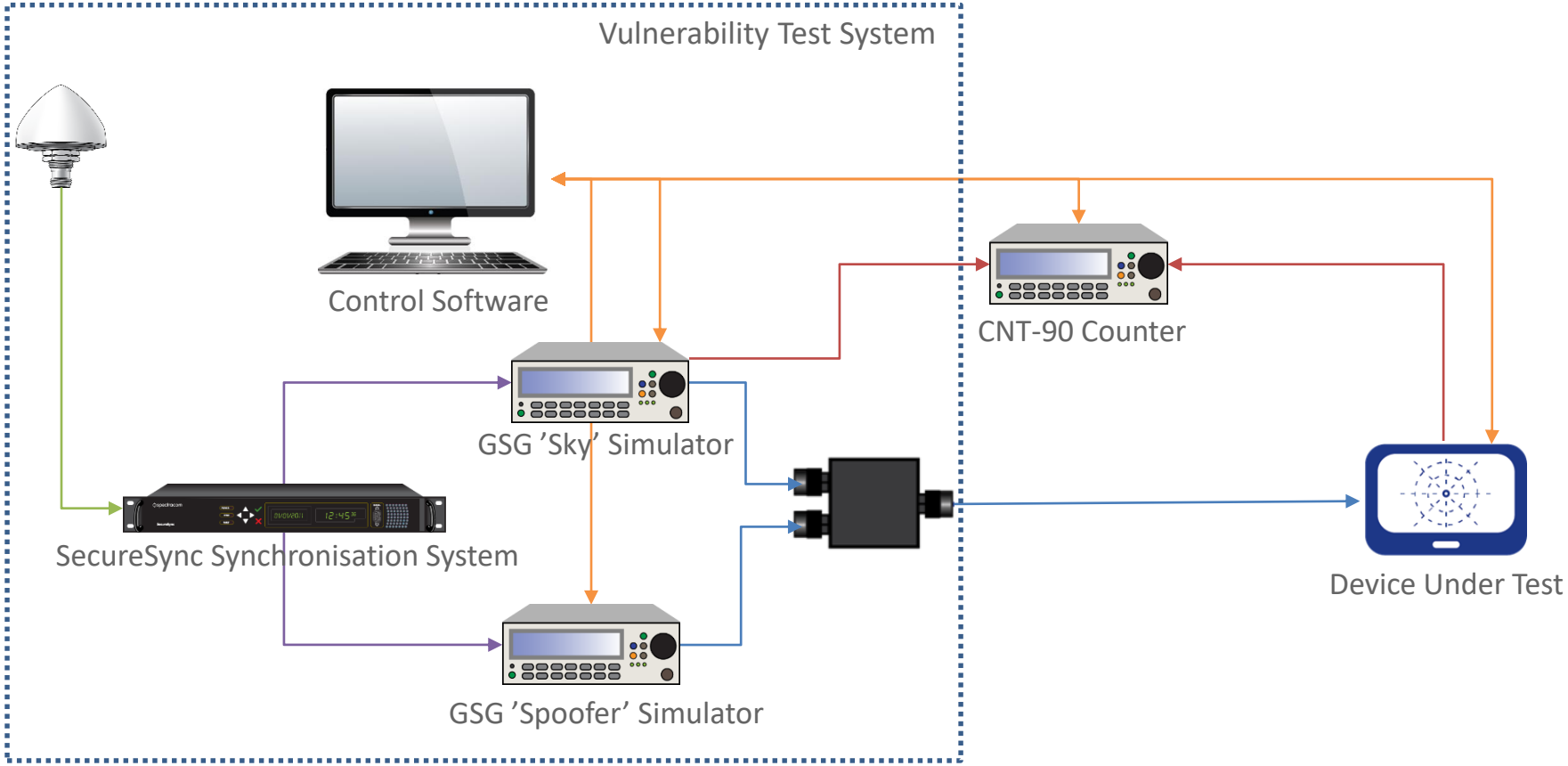
JAMMING

- **Example:** Delivery trucks jammer, malfunctioning electronics
- **Impact:** Loss in precision, Loss of reception

INTENTIONAL SPOOFING

- **Example:** Intentional perturbation of the system
- **Impact:** Clock drifting, potentially silently

Test Configuration



Hardening GPS/GNSS Systems

What happens to your system if GPS/GNSS is interfered?

- Malfunction? Fault?
- Position drift?
- Time sync drift?

- Does it issue an ALERT
  or does it just FAIL SILENTLY?
- ***Which is worse?***

spectracom

Jamming Test

- How your system reacts to jamming ?
- What the jamming indicator is worth ?
- Do you receive the good alerts ?

- Example : CW jamming with 161kHz offset with J/S of 12.3dB can give a 31m bias which has a 100ns impact

Temporary Loss of GNSS Signal

- How your system reacts to temporary loss of GNSS Signal ?
  - Antenna loss
  - Solar event
- What is the accuracy of the system when in Holdover ?

- Example : Simulate full GPS loss for 1h, and measure the real-life accuracy of the timing system

GNSS Perturbations

- Are you able to test your system against past events ?
- Are you able to test leap seconds ?

- Example : Replay the january 27th event (13,7µs jump) to qualify grandmasters

Additional Tests

- Behavior in multi-GNSS cases
- How long does it take to come back to initial performance ?

Example Test Cases

TIME Offsets

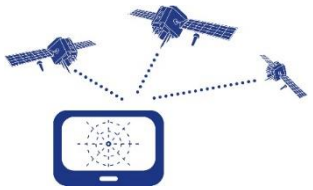
- 1ns
- 100ns
- 500ns
- 1.5usec

FREQUENCY Offsets

- $1{,}7e^{-8}$
- $2{,}3e^{-8}$
- $3{,}3e^{-8}$
- $5e^{-8}$
- $6{,}7e^{-8}$

POWER LEVEL Offsets

- +0dB
- +2dB
- +5dB



Multi-GNSS

- GPS-only
- Multi-GNSS

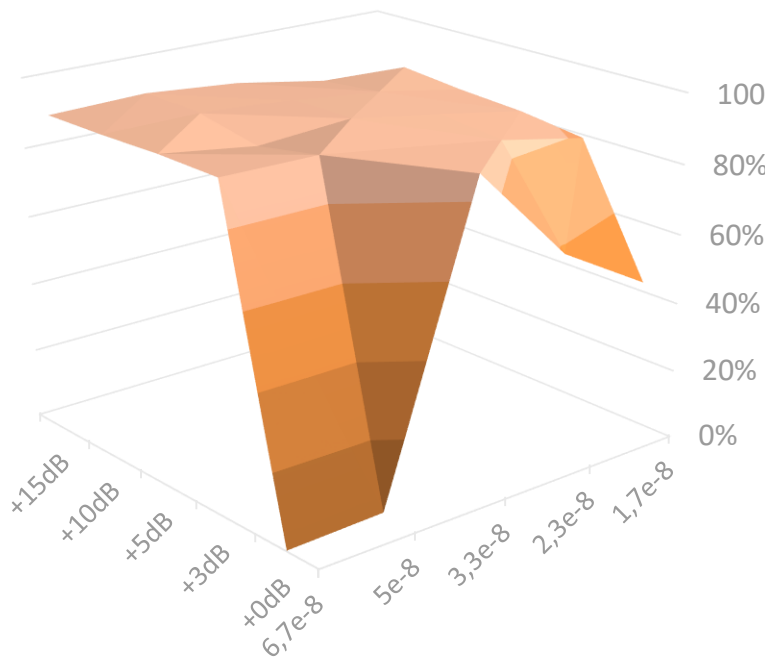
spectracom

Frequency Offset vs Power Above Sky

- Standalone GNSS receiver
- Different frequency offsets
- Different values of Power
- After 20s, we calculate a note to evaluate the spoofing

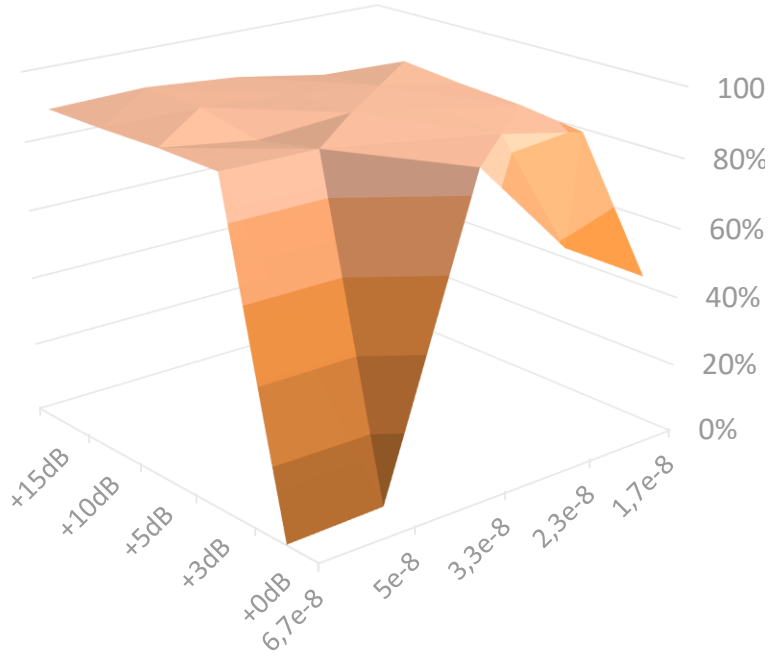
$$N = \frac{Offset_{meas}}{Offset_{th}}$$

- 100% means that the receiver has been totally spoofed



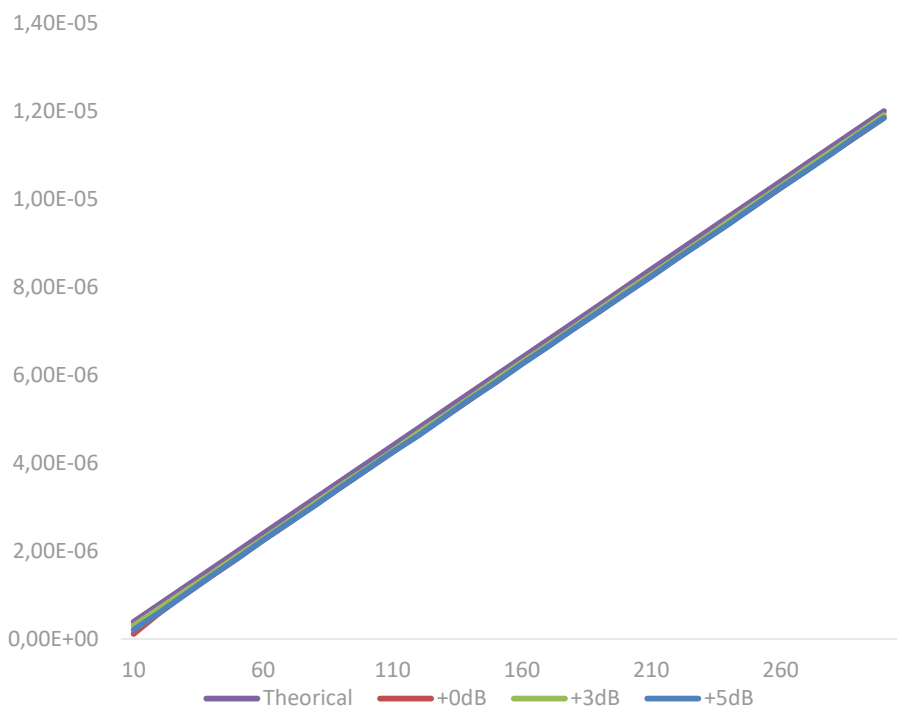
Frequency Offset vs Power Above Sky

- Power Above Sky can be 0dB
- No need for very high power
- Will depend on the Receiver Brand/Model
- No Alarm or Fix Loss !



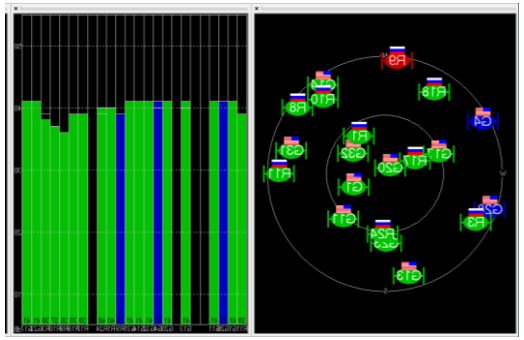
Impact of a Frequency Offset

- Run the test for 300s with a frequency offset of $3{,}3e^{-8}$
- We take a measurement every 10s
- We compare time offset vs theoretical time offset
- We run the test at different power above sky

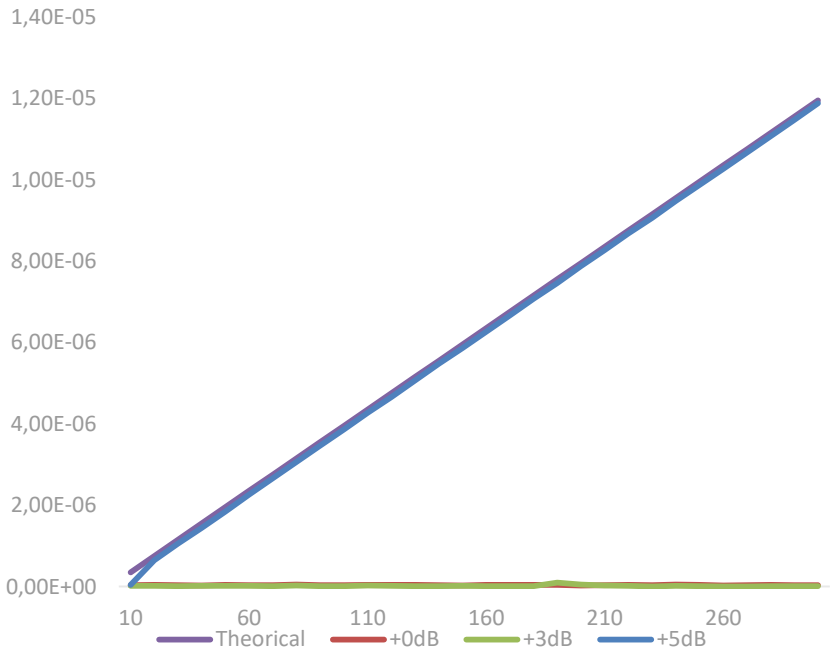


Impact of a Frequency Offset (with multi-GNSS)

- Re-run the same tests but
  - Sky is simulating GPS + Glonass
  - Spoofer is GPS only



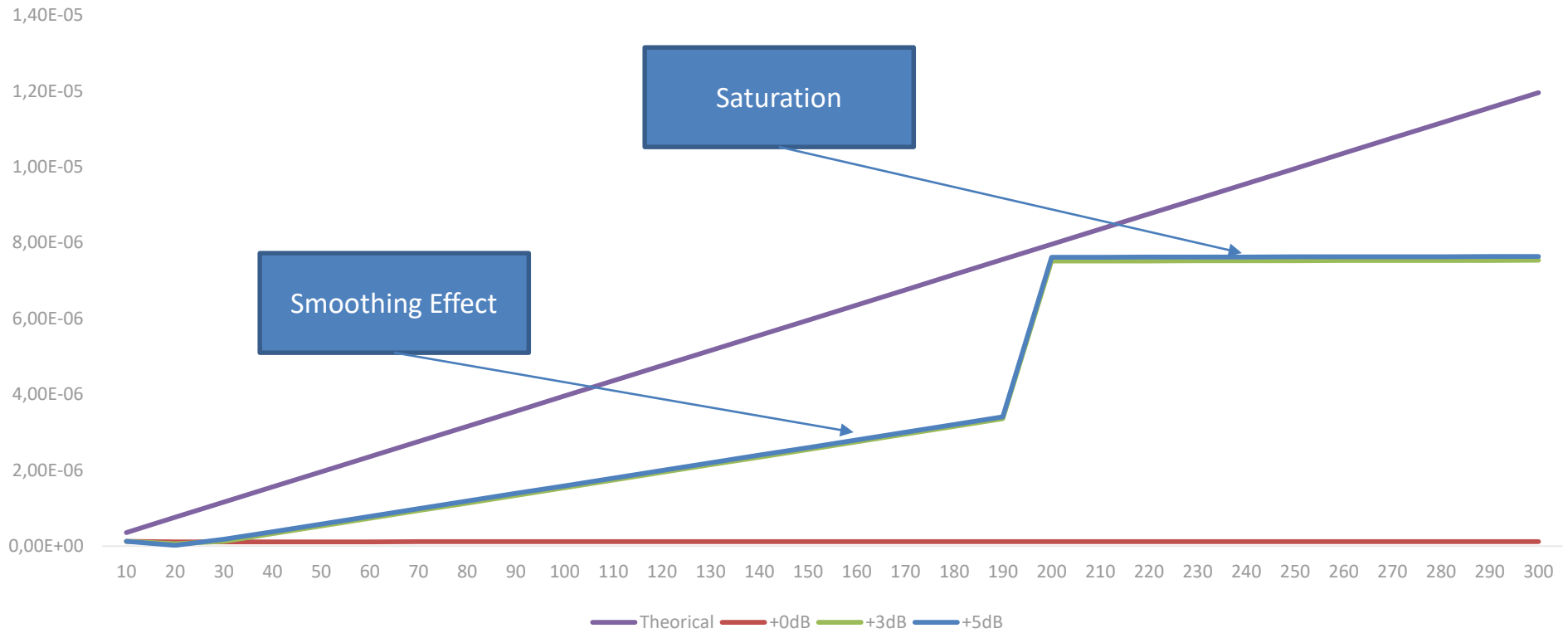
- Requires more power
- Not an ultimate solution



Impact of a Frequency Offset (with disciplined oscillator)

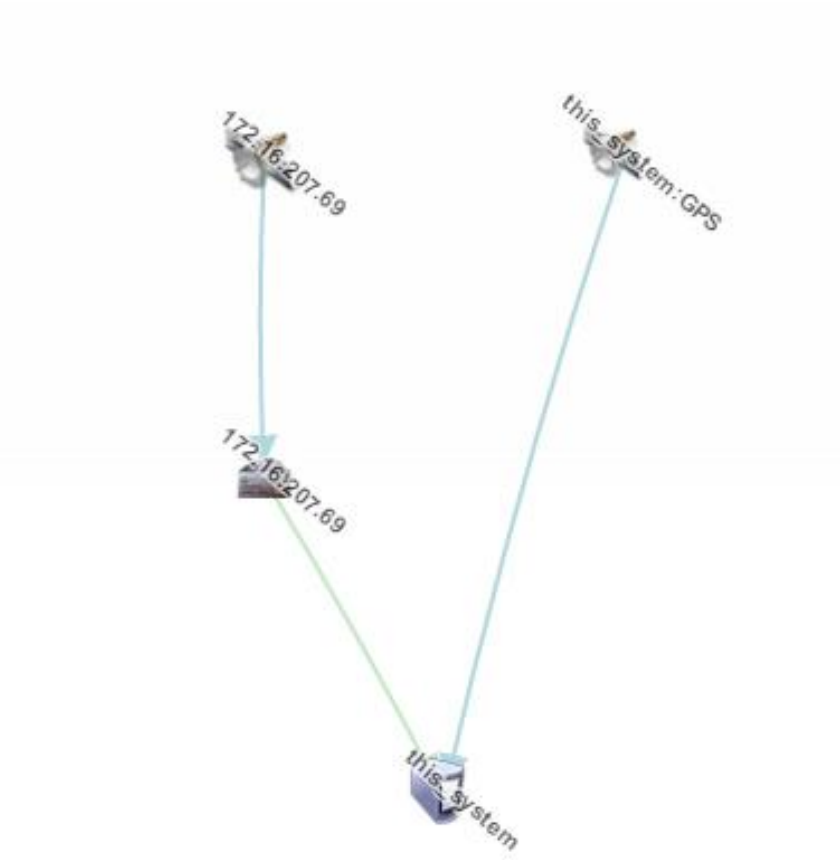
- Re-run the same tests in GPS only
- The GPS Receiver disciplines a Rb oscillator
- We compare the disciplined oscillator output to the Theoretical offset

Impact of a Frequency Offset (with disciplined oscillator)



Impact of a Frequency Offset (with Full GM)

- The behaviour of the Grand Master is logged during the test
- A trusted external source is added as a comparision
- Test is ran at +5dB
- The behaviour of the GPS + Rb is now known



Time offset Vs Time (with Full GM)

spectracom

Take Aways

- Pure Time Offset is easy to detect
  - Can be harmful but well handed by high-end Grand Master
- It is possible and silent to spoof a GPS Receiver with a frequency offset
- It is best practice for a PTP Grand Master to have :
  - Time smoothing
  - High-end Oscillator
  - Multiple/Redundant Time Sources Cross Checking
  - Time Monitoring and Logging
- Full knowledge of your systems is essential to understand their behaviour

Questions ?

jean-arnold.chenilleau@spectracom.orolia.com