

“Toughen” Team

10 December 2014

# “Toughen” Scope

- “Toughen” is the ability for satnav receivers to reject or operate through contaminated or invalid inputs, including:
  - In-band or out-of-band interference
  - Invalid signals transmitted by satellites
  - Invalid signals transmitted by unauthorized sources (spoofers)
  - Space weather (e.g., scintillation)
- Toughen applies to all satnav signals

# December 2014 Focus

- Speakers: financial transactions, agriculture, telecommunications & a leading receiver manufacturer.
- Pre-loaded questions for all:
  - What kind of toughness do you think is important for the applications you serve?
  - How do you measure the toughness of the product (conceptually, but also spec and test)?
  - What kind of feedback do you get from customers about the need for toughness?
  - Do you see a need to be tougher, and if so what approaches are you thinking about?
  - What negative aspects (performance, cost, reliability) are associated with making your product tougher?

# Common Themes

- Many critical SatNav applications are fixed-station timing-applications.
- Today,
  - Need  $\sim 1$  ms time
  - Fall back to high quality clocks and/or NTP
  - Tend towards gradual service degradation when SatNav is lost. .
- Tomorrow,
  - They will need better time accuracy to support regulation, security & next level of capabilities. (e.g. syncho-phasors for power and time stamps for all steps in financial transactions.)
  - These need  $\sim 1$  usec time.
  - Fall back to PTP, dedicated fibre, Ru, CSC,
  - Should also toughen the use of SatNav.
- We have time to do it, but lets start

# Recommendations

- NCO: document & disseminate best practices for toughening: (e.g. antennas, receiver processing, inertial measurements, smarter integration with augmentations.)
- DoD and DoS: re-evaluate ITAR limitations on deployment of well-known toughening techniques. For example, we need consideration of AJ & AS antenna technologies for aviation.
- FAA: ask NIST to examine the use of Schnorr signatures for SBAS/GPS authentication.
  - signature length compatible with SBAS & GPS
  - reputed to be unbreakable through 2030