

The Application and Limitations of GPS in Military CIS

Craig Benson
UNSW@ADFA

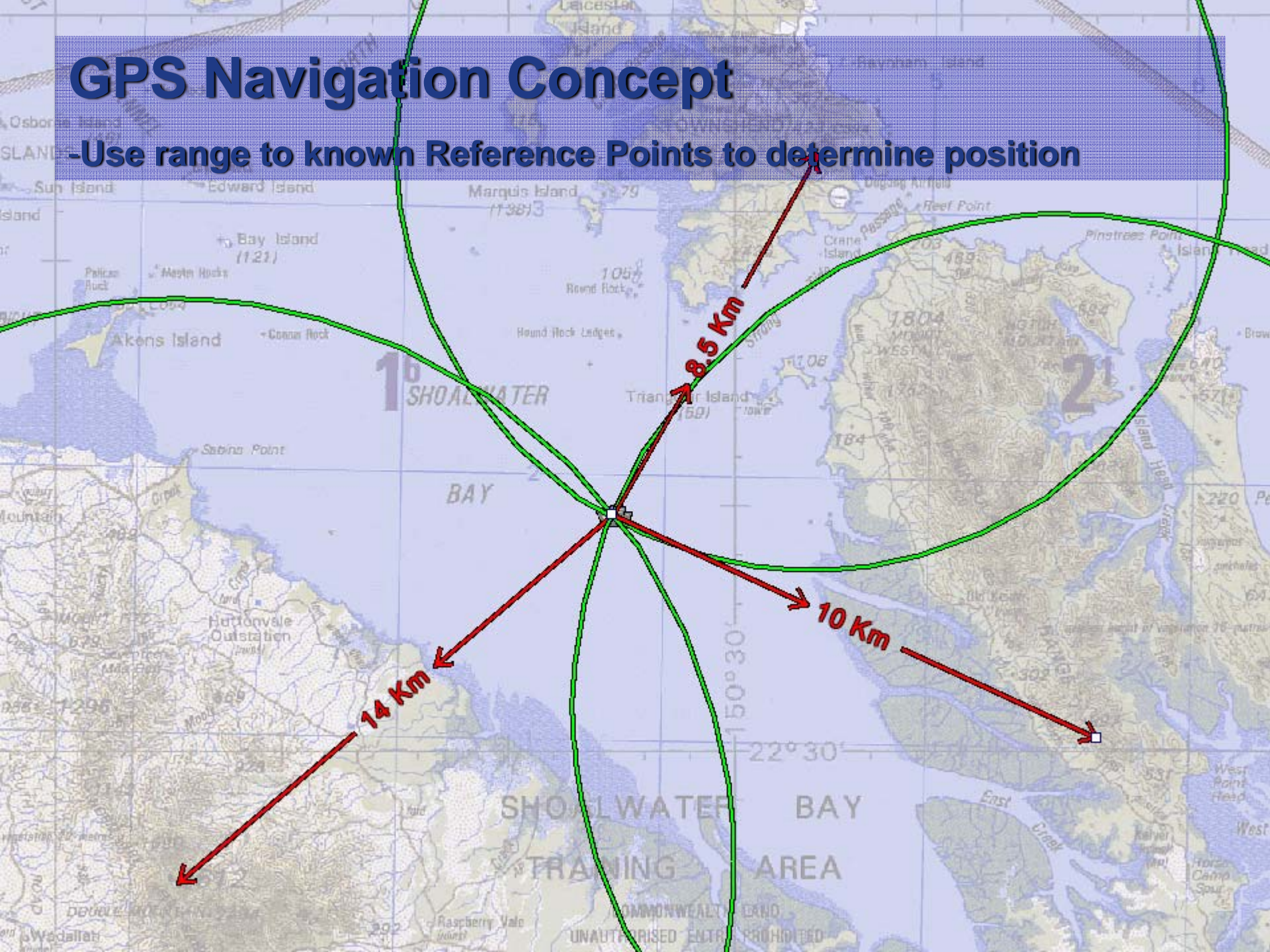
Introduction

- What is GPS?
 - A navigation & timing system
 - Provided by USAF
- What is it used for?
 - Navigation & Positioning
 - Timing
 - Orientation



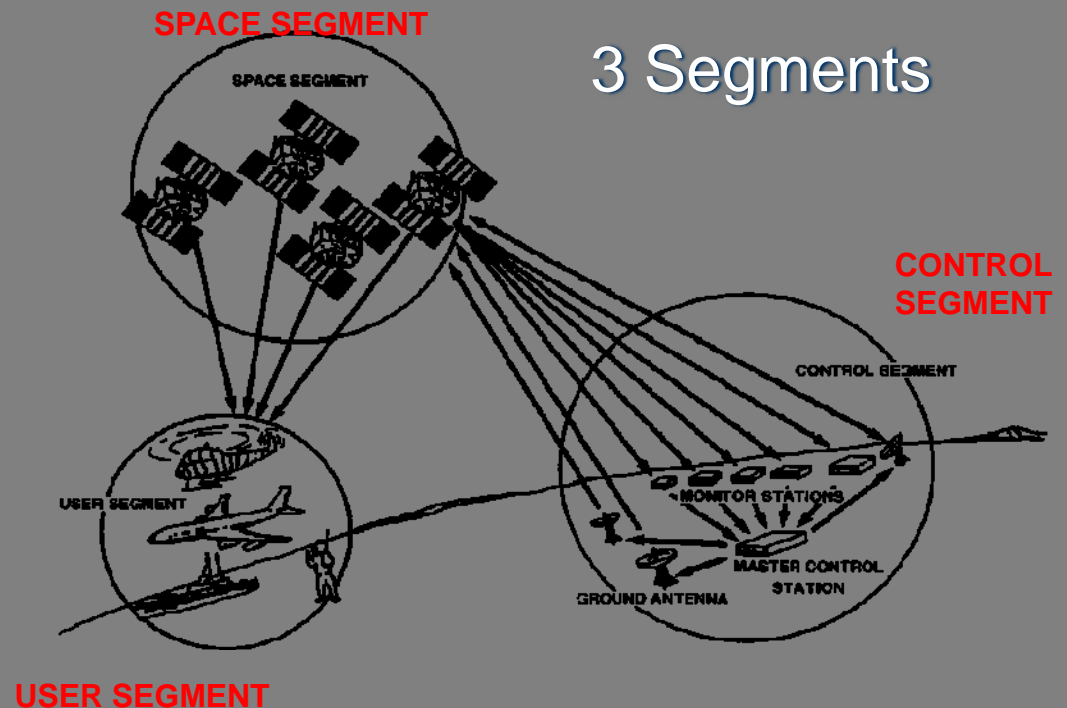
GPS Navigation Concept

-Use range to known Reference Points to determine position



GPS System Overview

- Primarily used for accurate world-wide navigation
- Two levels of service - SPS and PPS
- Three segments, we focus on the User Segment



Why is it used?

- Cheap
- Accurate
- Reliable
- Uniform
- Cheap

How does it fail?

- Loss
 - Tunnels and Urban Canyons
 - Jamming
- Errors
 - Multipath & software issues
 - Spoofing (deceptive jamming)

What are the implications of failure?

- Mission criticality
- Backups
- Blended solutions
- Graceful Degradation
- But look at reasons for use

User Segment

- Represents the key component for Military and Civil users to access NAVSTAR
- Military Users represent less than 1% of the NAVSTAR Users
- Civil GPS equipment capabilities developing quickly with military equipment technology falling behind
- Timing Applications Represent significant part of the user segment
- GPS Equipment is also referred to as HAE, Host Application Equipment
- Foreign Militaries require Memorandum of Agreement with the USA for access to Precise Positioning Service



Military Applications of GPS

- Navigation
- Blue Force Tracking
- Survey
- Gun / Mortar Alignment
- Targeting Sensors
- Weapon Guidance
- Timing
- Logistics Tracking
- Aviation
- Clearance Divers
- UAVs

Navigation

- Handheld
 - Position
 - Moving map
 - Time
 - Routes & Waypoints



Navigation

TomTom One \$279

- Vehicle
 - Position
 - Steer-to
 - Waypoints
 - Readability
 - Voice Interface



VPLGR ~\$7,000



Blue Force Tracking



FBCB2 in
HMMWV
(GPS is the
beige brick)
(USArmy photo)

Gun / Mortar Alignment

- Dual/single PLGR system
 - Dual receiver system provides sub-mil alignment for artillery
 - Single receiver provides several mils for mortar
- Standard feature for DAGR
- Makes indirect fire capability vulnerable to GPS loss



Targeting Sensors

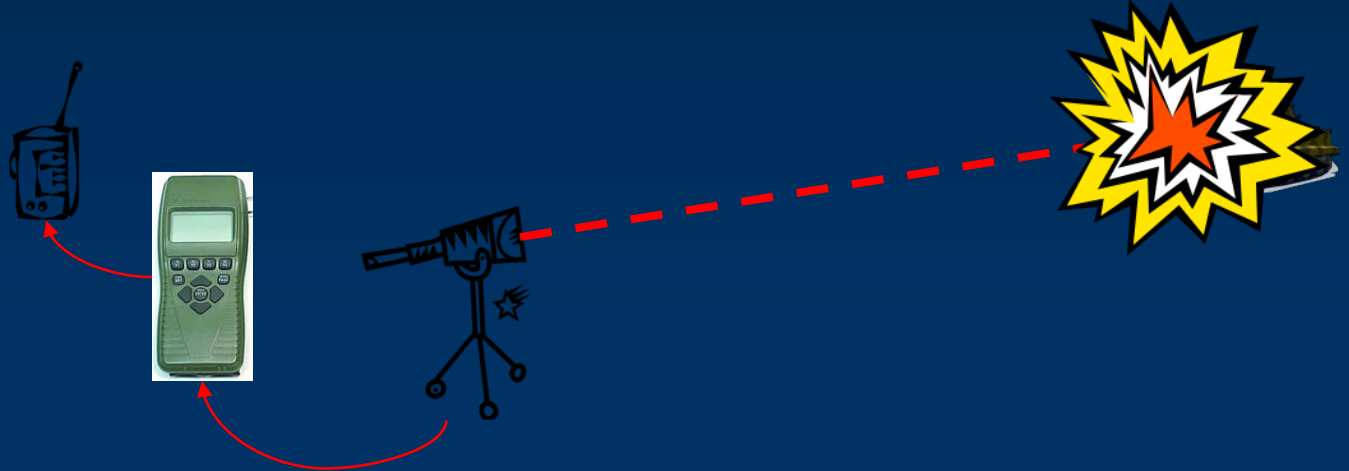
- Most battlespace nodes are capable of producing targeting quality data
- GPS provides own position
- Laser rangefinders provide range
- Flux compass normally gives bearing



Targeting Sensors



- Advantage of GPS / LRF automated systems is potential for elimination for voice relay and data re-entry



Timing



- Timing for time-stamping
- Synchronising secure radios
 - Have Quick
- Synchronising communications networks
- Frequency standards

GPS and Network Centric Warfare

- GPS underpins many of the advantages of a networked force
 - Blue force tracking requires automated, accurate positioning
 - Sensor to Shooter links need a common reference grid
 - Faster engagement cycles need accurate data from reconnaissance and surveillance assets
- Communications may also inherit GPS reliance

GPS and Advancing Technology

- GPS receivers have become very cheap and powerful
- Military systems lag behind
 - Security
 - Production volumes
 - Slow procurement cycles
- Threat systems may evolve faster and obtain more benefit than we will

GPS Signals

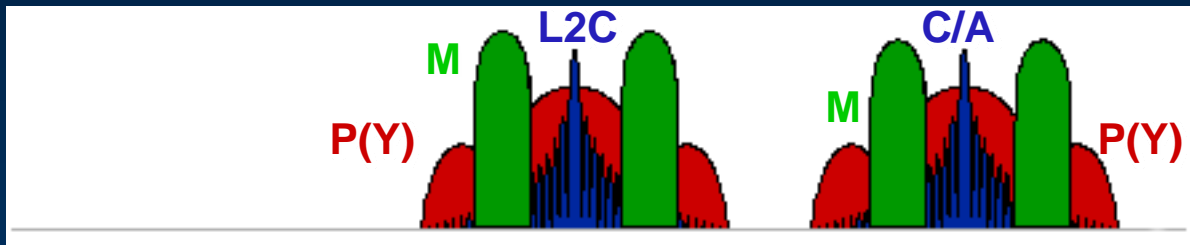
- 2 frequency channels L1(1575MHz) & L2(1227MHz)
- Each frequency has 2 logical spread spectrum signals Course/Acquisition and Precise
- *C/A code* is publically described, and is often referred to as 'civil code'.
- Precise *P-code* is the high performance signal
- It is now encrypted, and is referred to as *Y-code*, also known as 'military code'.
- Access to *Y-code* is restricted to authorised users and requires a special receiver and current crypto codes
- *P(Y)-code* refers to either *P* or *Y-code*, which-ever is being transmitted

The Signals in Space

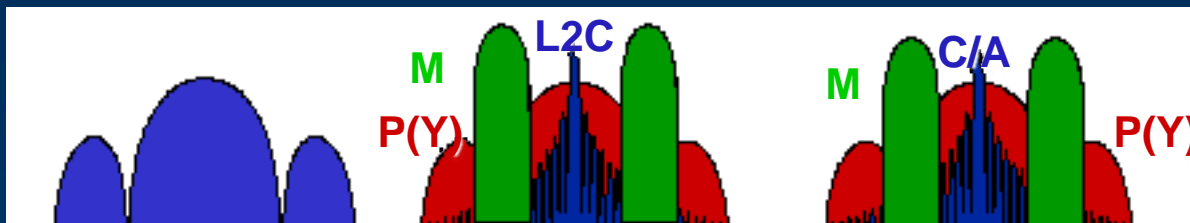
Block II/IIA/IIR



Block IIR-M



Block IIF (III)



L5
1176MHz

L2
1227MHz

L1
1575MHz

GPS Receiver Keying

- *Y-code* is an encrypted version of *P-code*
- It is not actually 'decrypted', rather the receiver generates *P-code*, encrypts it into *Y-code*, then uses this to correlate with the signal from the satellite
- The crypto key used to do this changes daily, and is known as Crypto Variable Daily (CVD)

GPS Receiver Keying

- GPS crypto is very valuable, so certain measures are taken to preserve it
- There are 2 security architectures for Y-code GPS receivers
 - PPS-SM
 - SAASM. Newer, so tends to be mated to more capable receivers. Many of the ‘advantages of SAASM’ are actually just ‘advantages of newer receivers’.

GPS Receiver Keying

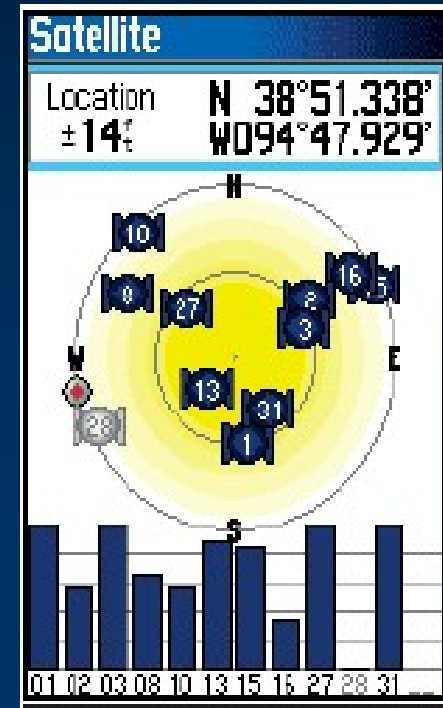
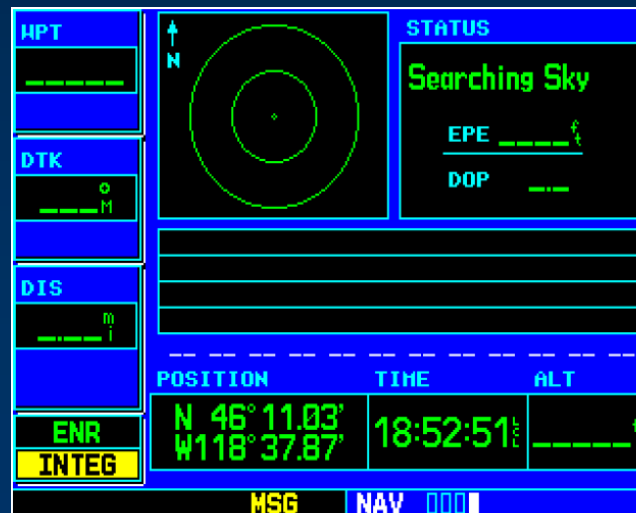
- CVD is never directly loaded into the receiver, instead key generation keys are used
- Crypto-Variable Weekly (CVW) allows a receiver to generate a whole week of CVDs
- Crypto-Variable Monthly (CVM) allows the receiver to generate a whole month of CVDs
- Group Unique Variable (GUV) allows the receiver to generate a whole year of CVDs, but only using additional data provided from GPS satellites every day.

GPS Receiver Keying

- Historically GPS keys were classified crypto-controlled items – so called **Red** keys
- The SAASM security architecture allows use of so called **Black** keys. These are unclassified and easier to handle
- SAASM is also designed to support ‘over the air rekeying’, meaning that standard GPS receivers key themselves by downloading data from satellites.

Performance Measures

- Position Accuracy
- Velocity Accuracy
- Time Accuracy
- Time to First Fix
- Jammer Immunity



Accuracy

- DoD GPS Accuracy Specification:
- PPS
 - 10m CEP 95%, horizontal (Average ~ 3.1m)
 - 16m SEP 50%, vertical
 - ~ 97 nsec (4SV, low dynamic)
- SPS
 - 33m CEP 95%, horizontal (Average ~ 8.3m)
 - 73m SEP 95%
 - ~ 157 nsec (4SV, low dynamic)

Can also measure velocity by position change (or by doppler),
PPS - 0.2m/s per axis (95%), SPS (0.4 m/s)

- **Note that this data is based on the SPS Performance Specification and the averages are global averages**

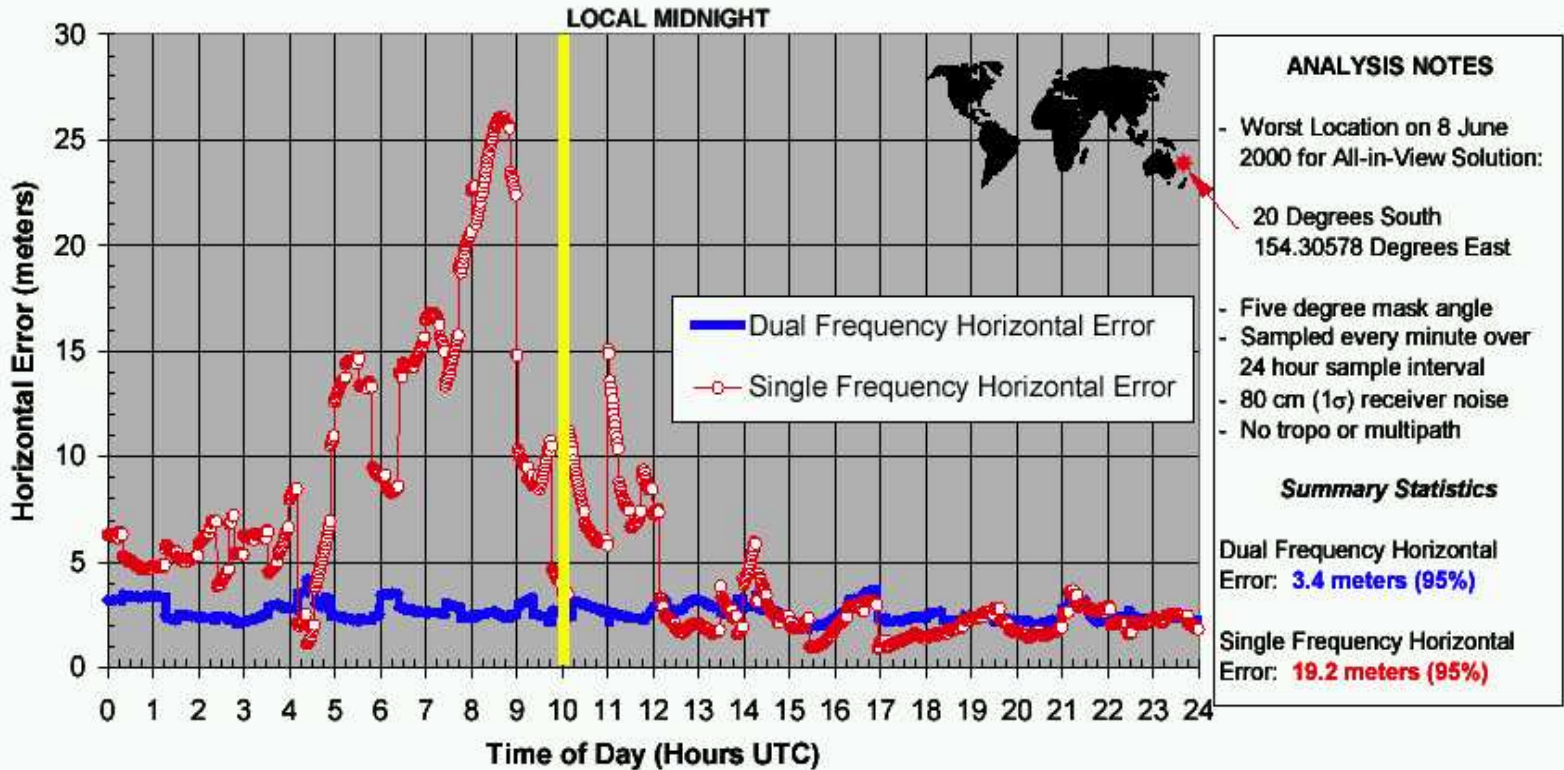
Civil vs Military Receivers

- Y-code capable receivers have several inherent advantages
 - Historically C/A-code could not provide ionospheric corrections, while Y-code could
 - Y-code has higher resistance to Electronic Attack (jamming and deception)
 - Y-code is marginally more accurate
- But C/A code receivers also offer advantages
 - Mass production means smaller, lighter, cheaper receivers, available in more pre-configured devices
 - C/A receivers typically use substantially less power

Accuracy

Source: GPS SPS Performance Standard, Oct

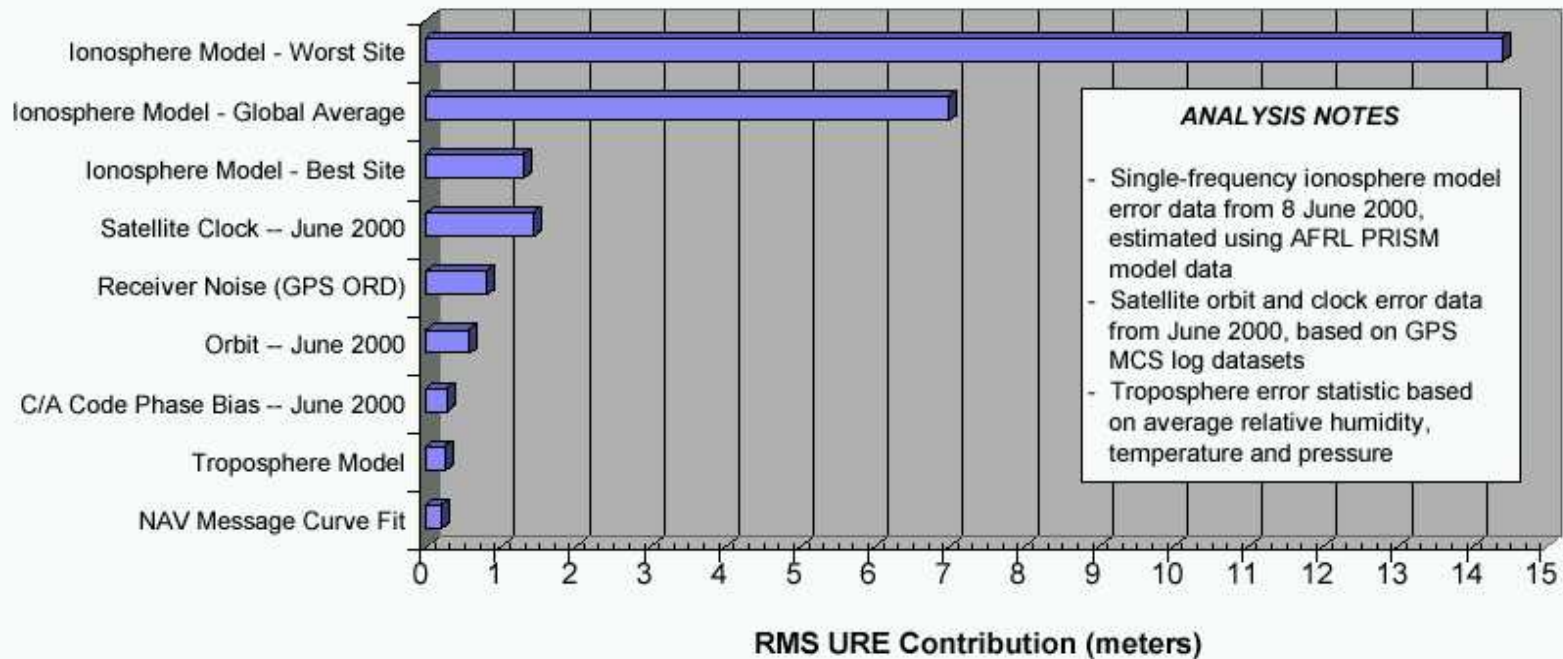
Comparison of All-in-View Single and Dual-Frequency Horizontal Errors
Worst Single-Frequency Performance Location, 8 June 2000



Looking at the Errors

Source: GPS SPS Performance Standard, Oct 2001

Elements of SPS User Range Error



Accuracy - Why Military Receivers are More Accurate

Propagation Errors



Ionosphere

$L1$

$L2$

$\Delta T1$

$\Delta T2$



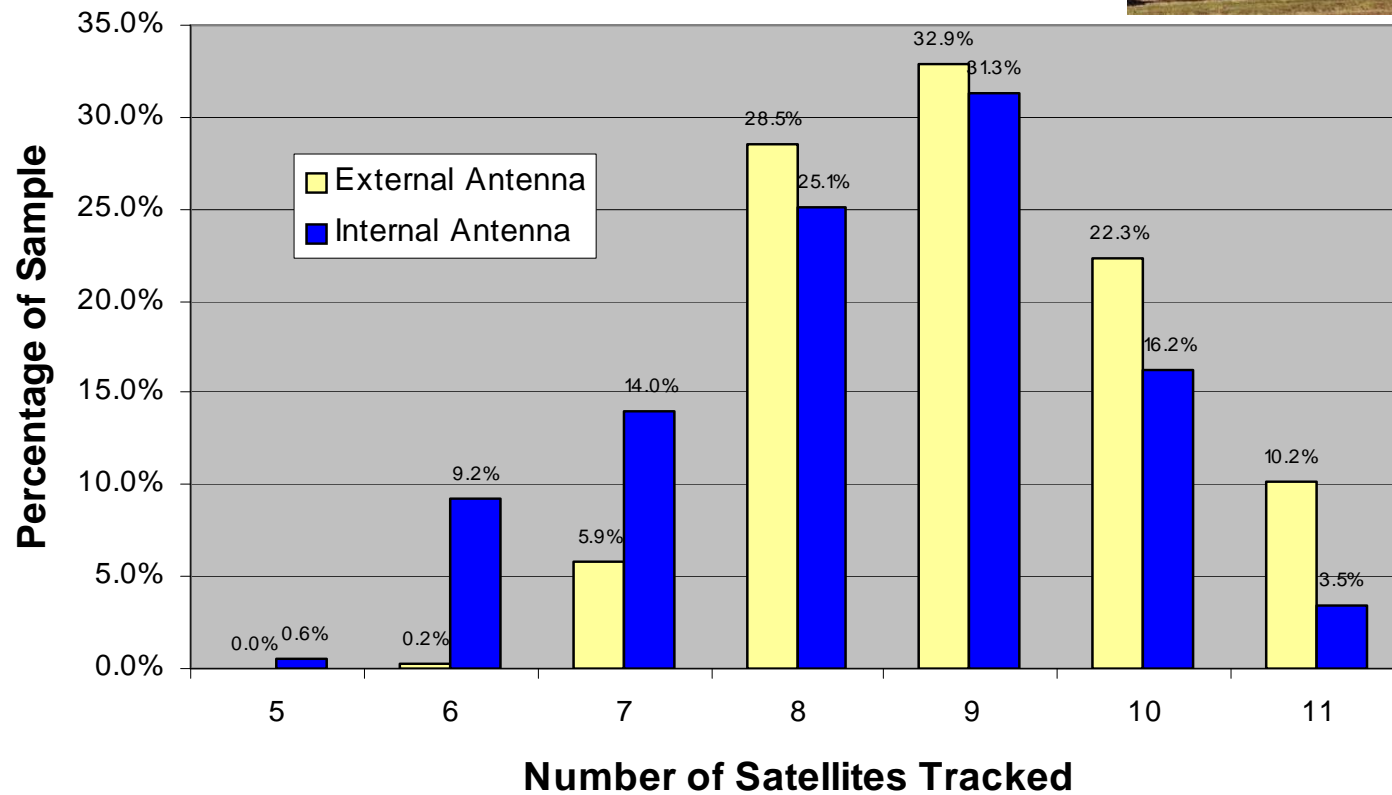
Propagation delay is different for the L1 and L2 frequencies. This can be used to partially correct for propagation error

The Ionosphere causes a time error, having 2 frequencies, L1&L2 allows some correction of this error

Availability

Kiowa Garmin III Pilot
Testing, Oakey, 2001

Antenna Sample Distribution (Using All Samples)



How does it fail?

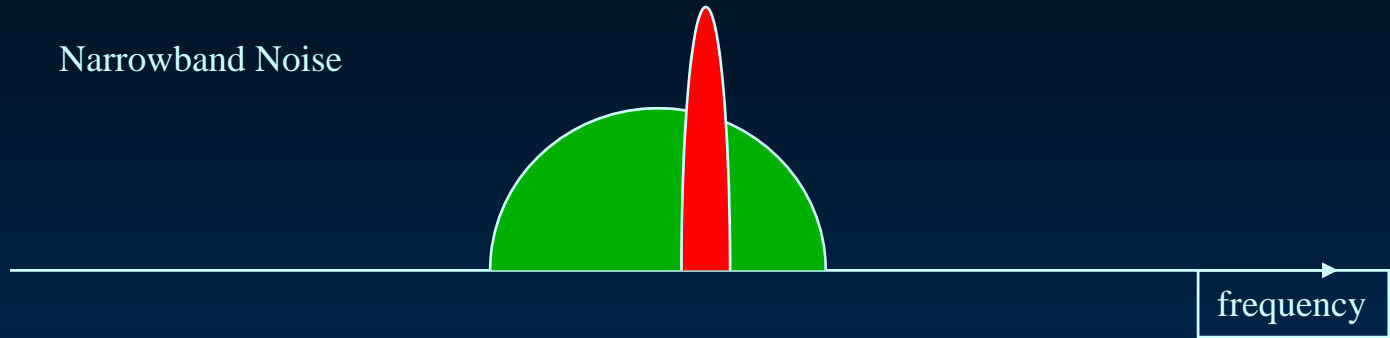
- Loss
 - Tunnels and Urban Canyons
 - Jamming
- Errors
 - Multipath & software issues
 - Spoofing (deceptive jamming)

Tunnels and Urban Canyons

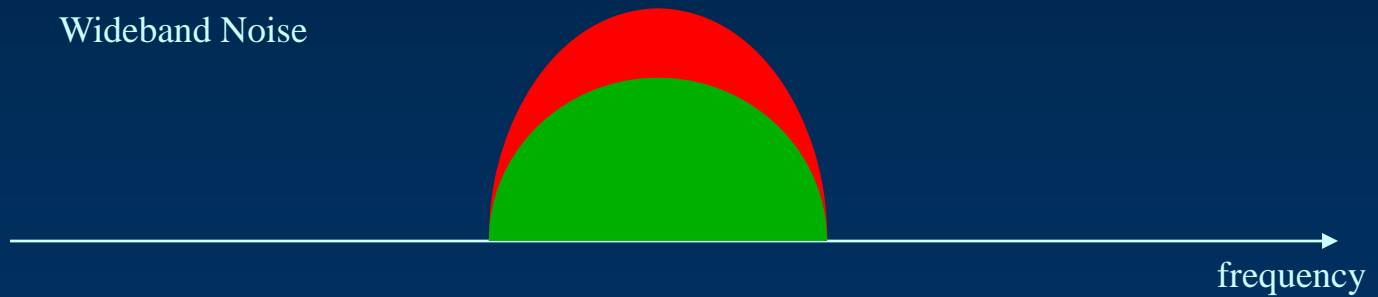


Noise Jamming

Narrowband Noise



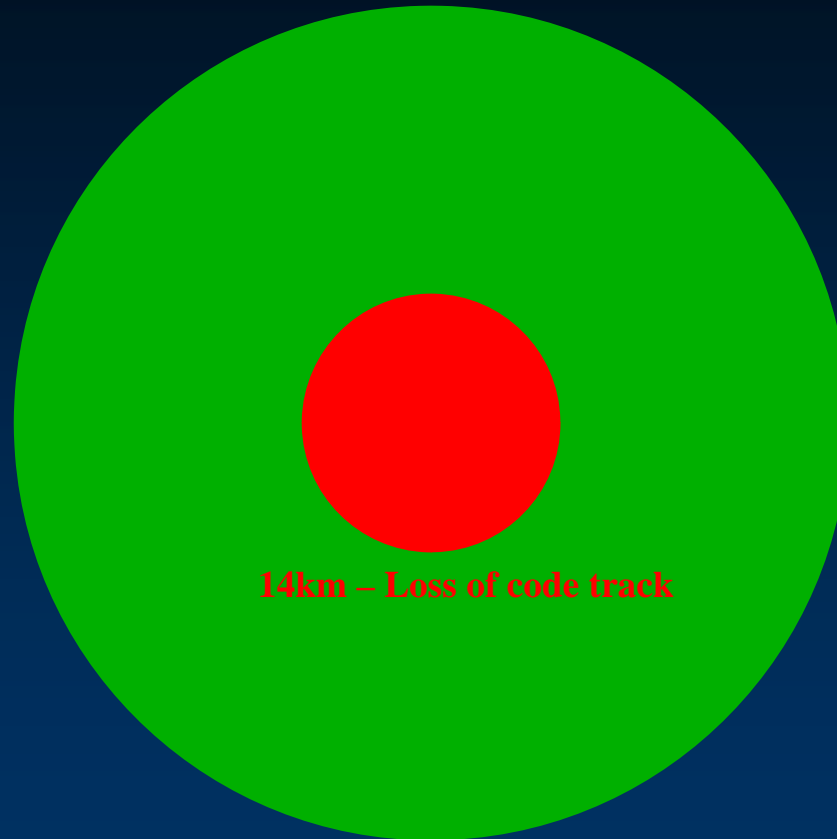
Wideband Noise



Effect of Noise Jamming

- Normally the signal quality in the GPS receiver is expressed at a Carrier to Noise ratio (C/N_0)
- N_0 is supposed to be noise (per Hz)
- If we expand our interpretation of Noise to be 'any unwanted signal', then this includes the Jammer
- A Noise Jammer then adds to N_0 , and our C/N_0 ratio drops
- For very low jamming levels, the noise floor dominates – and jamming has no effect
- As the jamming gets stronger, it dominates. For every doubling of jammer power (3dB), the C/N_0 halves (-3dB)

Jamming Ranges – 1W jammer



14km – Loss of code track

44km – Loss of carrier track

From: Owen on www.rin.org.uk

Typical GPS Jammers

National Air Intelligence Center, AIA

Unclassified



Unclassified

7737015697

F-186601

Aviaconversia Jammer c1997

Photo from http://www.qsl.net/n9zia/wireless/gps_jam-pics.html

Commercial

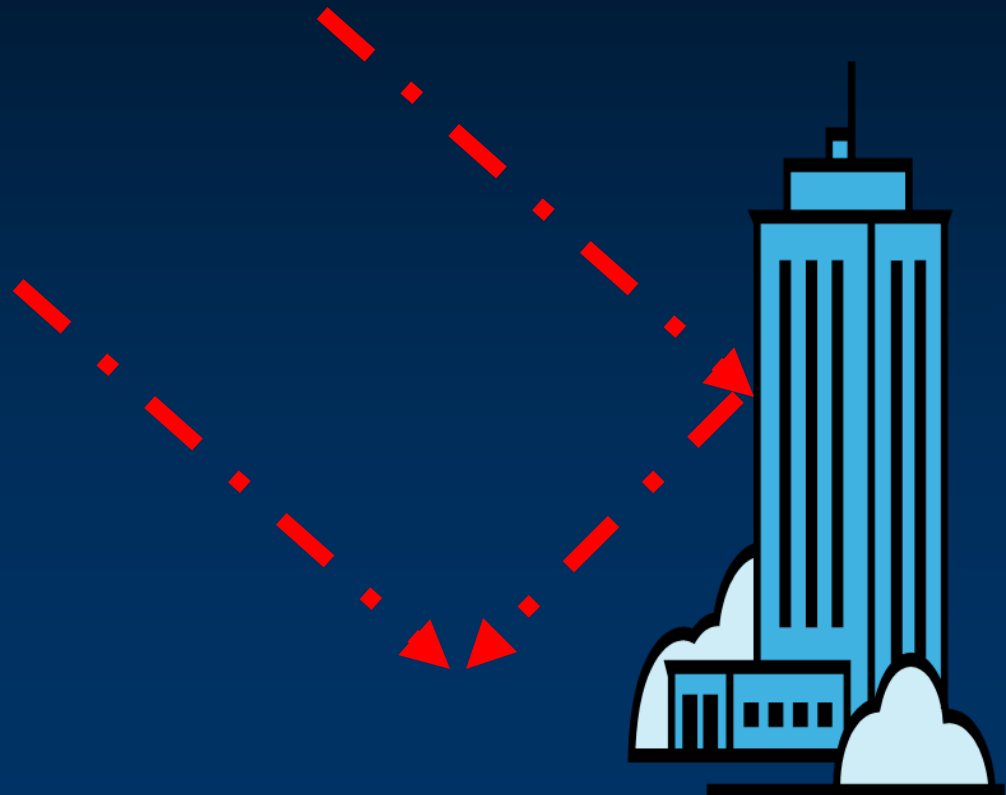
- 1W radiated power
- Jamming claimed
 - Up to 50km



Photo from <http://www.grove-ent.com/rac02.html>

Multipath

- Reflections off terrain and structures



Deception Jamming

- A jammer can transmit a GPS-like signal
 - For C/A-code, can generate a fake signal
 - Spoofing
 - For Y-code, can rebroadcast signal
 - Repeater Jammer

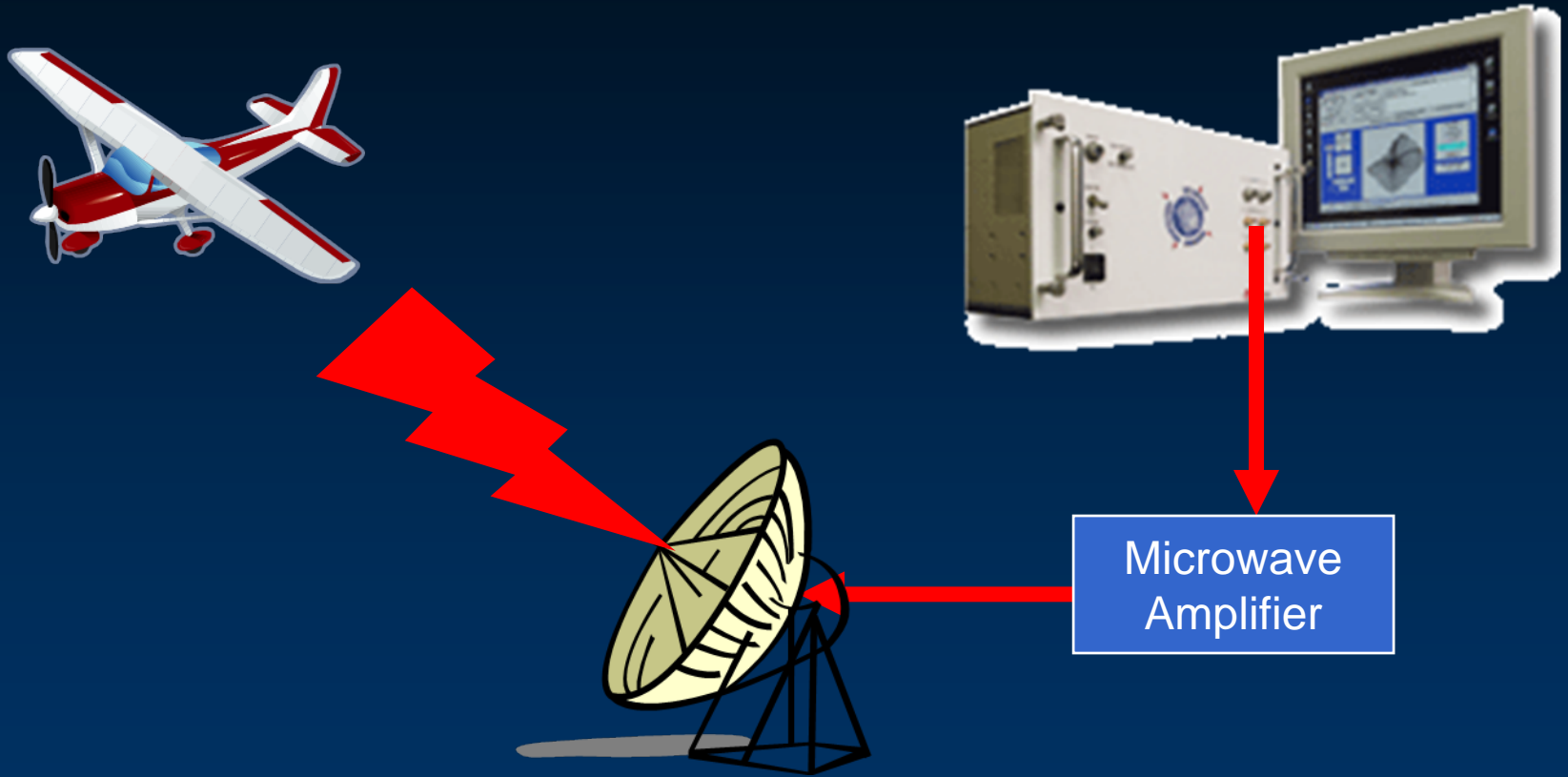
Spooftng

- Commercial satellite simulators are available
- These are designed for use as lab test equipment to test GPS receivers
 - Generate artificial satellite constellation
 - Provide a notional receiver location
 - Output an RF signal to feed to GPS receiver antenna port

GPS Satellite Simulator



GPS Spoofer



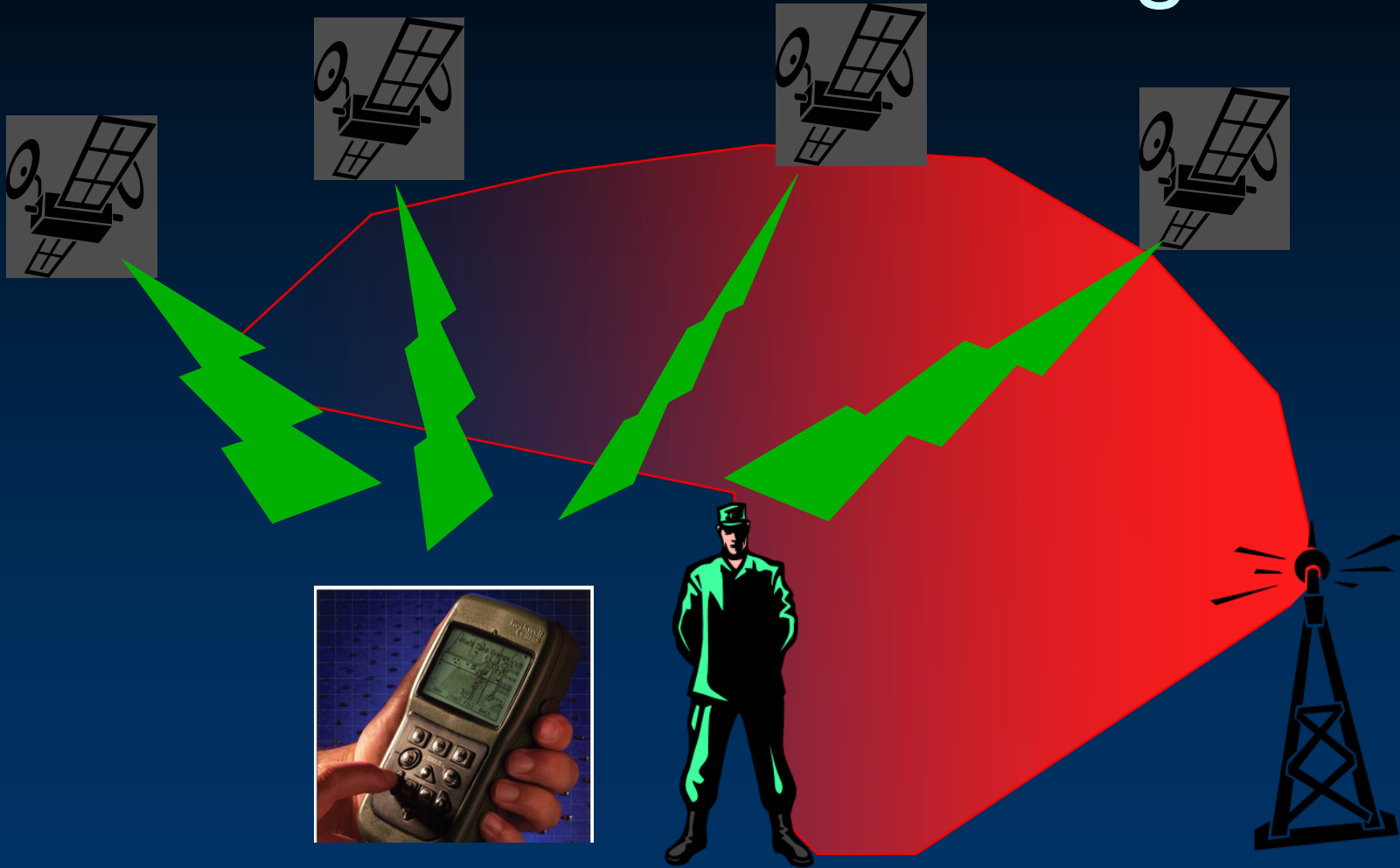
GPS Receiver Protection

- GPS receivers can be protected from jamming to some extent. Protection methods include:
 - Shielding
 - Ground Planes & Choke Rings
 - CRPA
 - Filters
 - Blending with Inertial Sensors

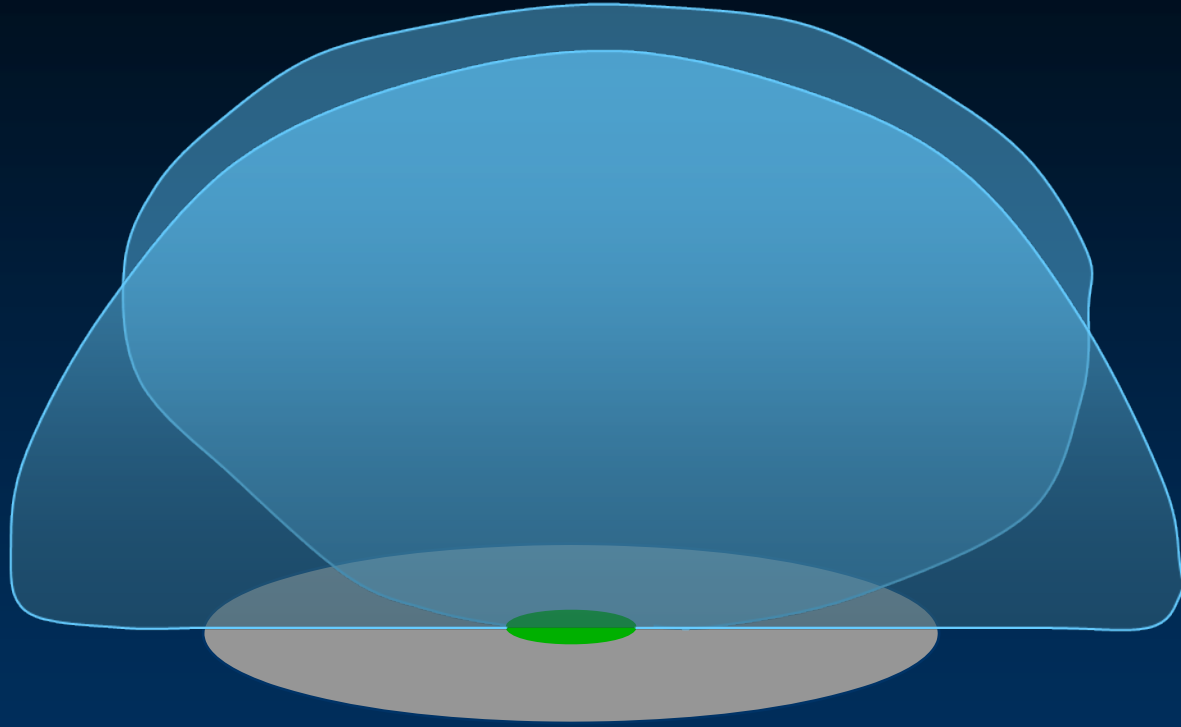
Receiver Shielding

- Buildings
- Human Body
- Terrain
- Shell Scrape

Receiver Shielding



Ground Planes



Choke Rings

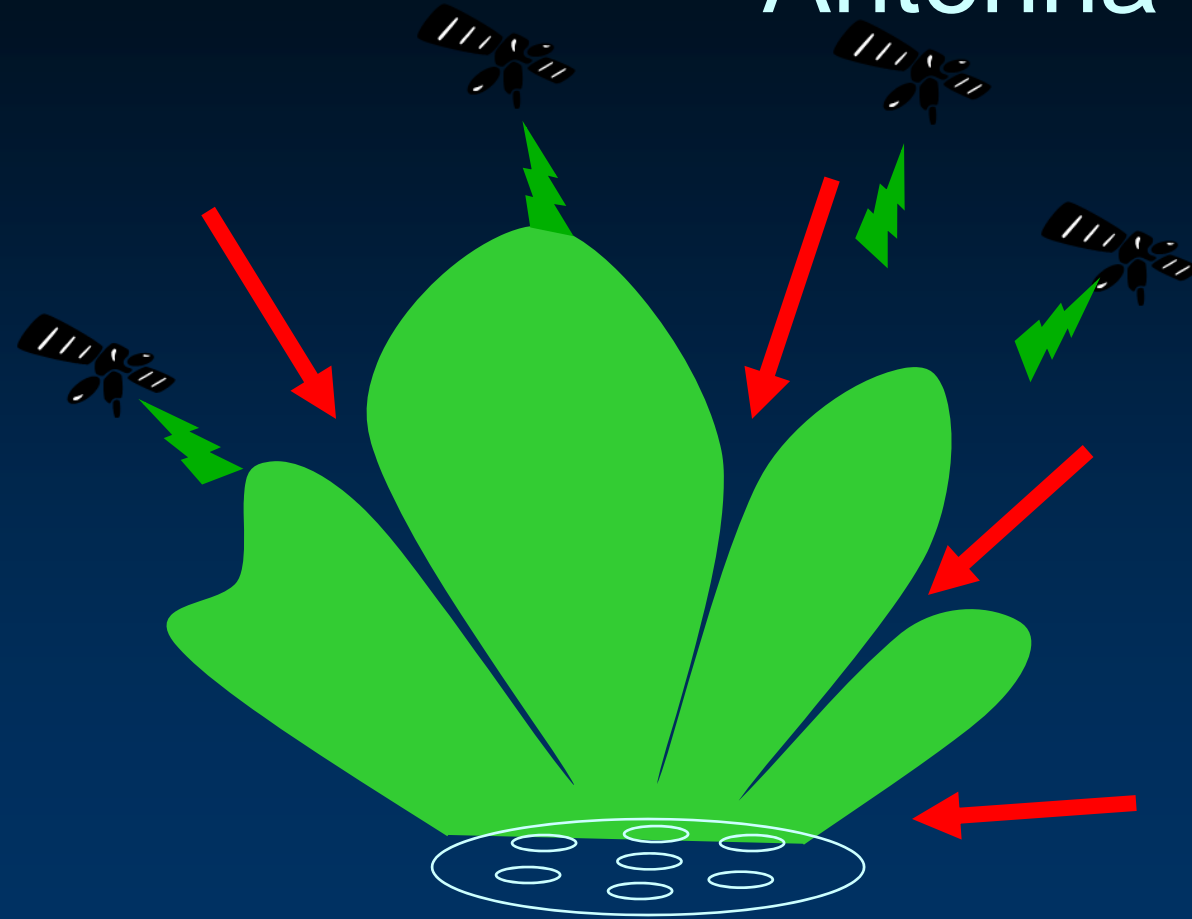
- A Choke Ring is a fancy ground plane that performs even better attenuation of low elevation signals
- Used by some GPS professionals (eg Surveyors) to eliminate multipath signals

Choke Rings

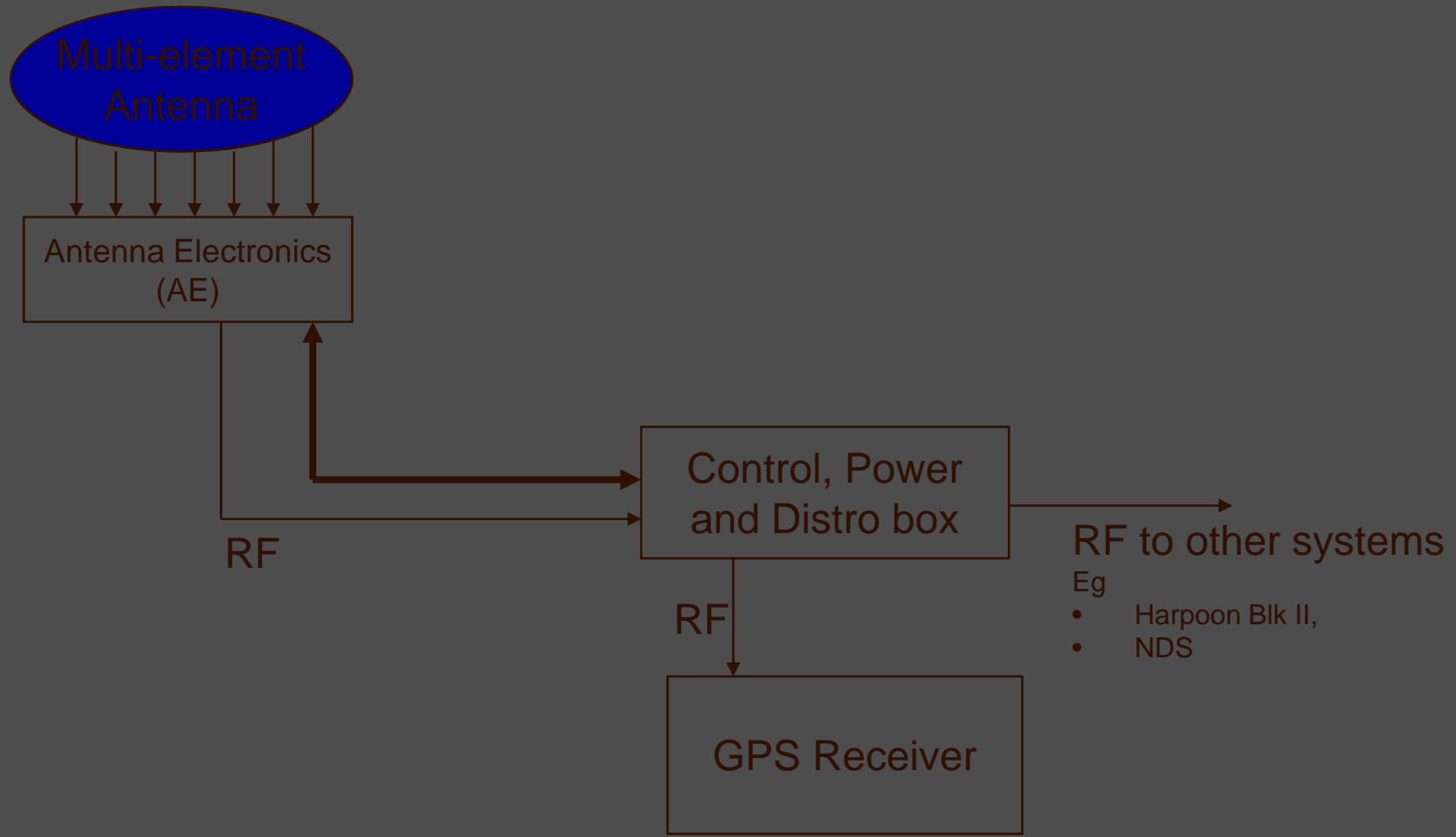


Choke Ring used by Surveyors
Photo: Trimble

Controlled Reception Pattern Antenna

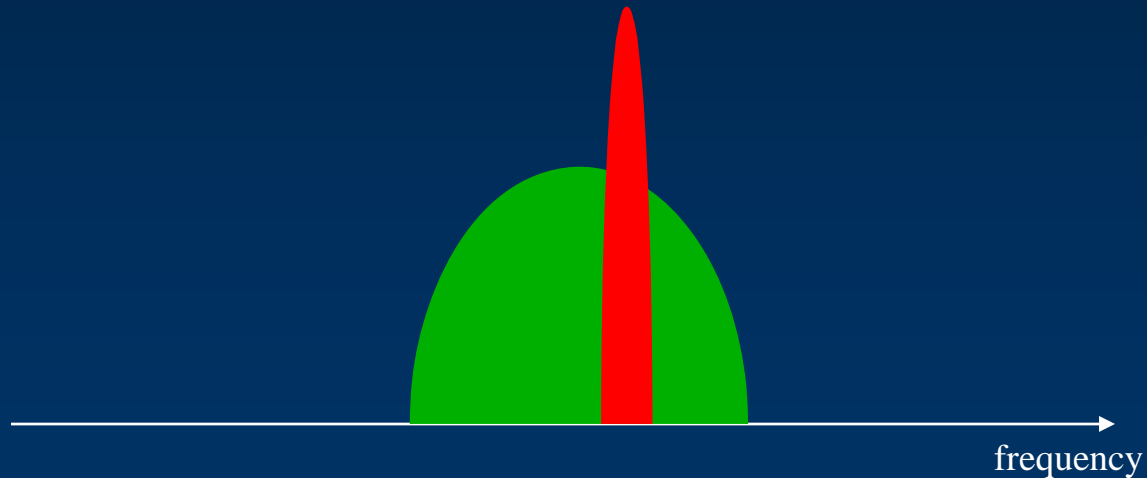


CRPA Platform Installation

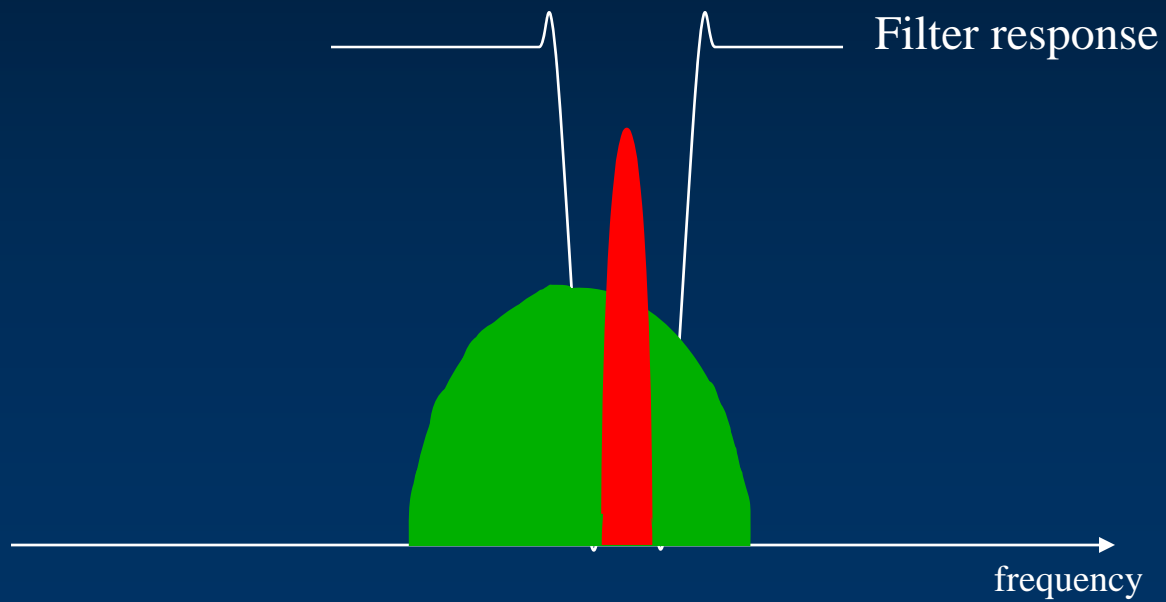


Filters

- Some filters are available to minimise jamming
- Frequency selective filters
 - Notch out the jamming



Filters



Frequency Filters

- Track & adaptively minimise interference
- Partial removal of GPS band has only a proportional effect on GPS signal level
 - Remove 20% of band = 80% of power left

Alternates to GPS

- Other Global Navigation Satellite Systems (GNSSs)
 - GLONASS, GALILEO
- Alternate Radio Ranging Systems
 - Mobile Phones
 - EPLRs
- Inertial Navigation Systems
 - And other Dead Reckoning Systems
- Outside reference systems
 - TERPROM, Map Aiding, Waypoints

Other GNSSs

- **GLONASS**
 - Soviet GPS-ski
 - Military inspired
 - Limited satellites (17 operational)
- **GALILEO**
 - European GPS copy
 - Commercially inspired – state sponsored
 - Deployment from 2010?

Other GNSS facilities

- Most other GNSS systems are GPS enhancement services
 - WAAS – US wide area differential
 - EGNOS – EU wide area differential
 - MSAS – Japanese wide area differential

Alternate Radio Navigation

- Mobile Phone towers can assist cellular users with navigation
- Military systems such as EPLRS can provide a similar capability
- Navigation is then relative to the radio source
 - Mobile phone towers can be surveyed
 - Military tactical radios there will have some error

Inertial Navigation Systems

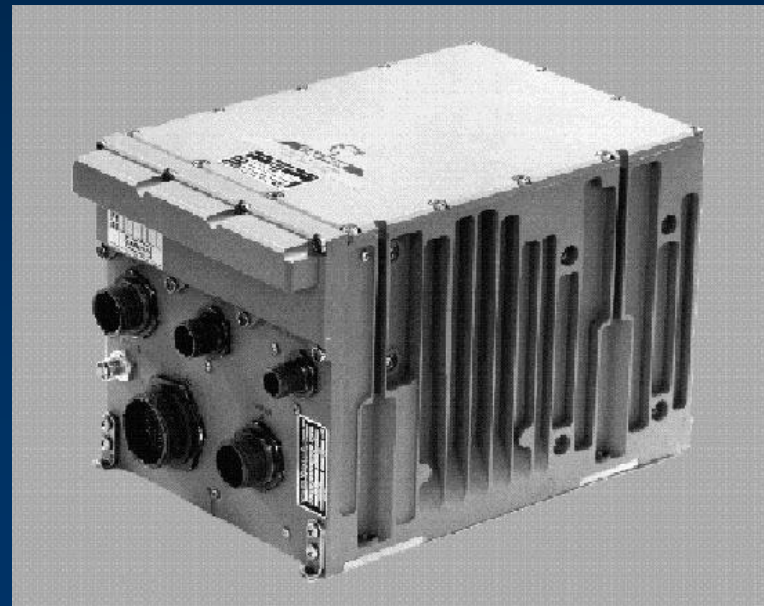
- 3-axis gyroscopes
- 3-axis accelerometers
- Measure acceleration vectors
- Integrate to get velocity vectors
- Integrate to get position
- Totally self contained navigation!

Inertial Navigation System Limits

- Small acceleration errors accumulate into velocity errors, and then again into position errors
 - Manage these by taking a speed input. Accuracy of speed input not especially important
- Need alignment
 - Historically stationary, but now normally moving – using GPS

Embedded GPS INS (EGI)

- GPS and INS in a single box
 - GPS calibrates the INS whenever GPS is available – in-flight align
 - INS provides initial position to GPS, and other aiding



Alternates to GPS

- Map navigation skills
- Map Matching for on-road vehicles
- TERPROM
- Atomic Clocks

Map Aiding

- If the body of interest has limited freedom, then this drastically simplifies the navigation problem
 - Trains on rails
 - Cars on roads
- Knowledge of the possible lines of movement allows correlation of map data to very low quality gyro and odometer feeds to provide position fixes
 - Doesn't even require start point
- These techniques are not a poor quality inertial, rather they navigate by watching the tissue box slide back and forth across the rear parcel shelf of the car

TERPROM

- TERPROM is a BAE Systems insert into an aircraft Inertial Navigation System
- It compares the terrain rising and falling under the aircraft with a stored database (DTED)
- This allows it to determine the aircraft location and trajectory
- As a bonus it can predict Controlled Flight Into Terrain (CFIT)

Atomic Clocks

- Atomic Clocks are a form of clock that has very good long term accuracy (1×10^{-12})
- They can therefore condition frequency standards and network synchronisation to very high accuracy
- DARPA have developed very small atomic clocks to support future capabilities

Utility & User Acceptance

- User requirements include:
 - Reliable
 - Small
 - Light
 - User-friendly
 - Low power consumption
 - Rugged
 - ...
- By most of these metrics, civil receivers are superior to military ones
- In addition, the features of military receivers that are superior to civil receivers are often hidden from users
 - eg. protection from jamming is difficult to appreciate if users never experience jamming

Utility & User Acceptance

- We traditionally undervalue the ergonomics of military equipment
 - Witness the current weight burden on foot soldiers, although there is growing realisation of this problem
- The impact of a poor user interface cannot be underestimated



Canberra Canberra



Testing / complex systems

- Many of the systems discussed are complex systems that we did not design
 - Or for networks, we designed them but cannot fully understand them
- We may understand the conceptual way in which they are built, but we can not be sure how they will behave
 - Eg an EGI should be able to resist being walked off at more than its maximum rate of drift
- Testing is the only way to be sure

Conclusion

- GPS is a highly useful, even transformational tool.
- It is often adopted because nothing else can do the job in a way that is low-cost, small, light or accurate enough
- But it is very vulnerable. Civil users can often afford to accept the risk of GPS failure
- Military systems are normally more interested in 'worst case' performance, especially since the adversary can cause that poor performance
- But Military GPS receivers often perform poorly in most respects compared to civil receivers