GNSS Status and Vulnerabilities

ITSF 2011

1-3 November 2011

Marc A. Weiss, Ph.D.
Time and Frequency Division
National Institute of
Standards and Technology
mweiss@boulder.nist.gov/ ++1-303-497-3261

This Talk has Two Messages

1. GNSS are robust and growing and provide real-time UTC time and navigation in a $10B industry

2. GNSS signals are dangerously vulnerable to both accidental and intentional interference

Sync Sources: GNSS and Atomic Clocks

- **Intro: Time and Frequency Signals**
- **GNSS**
  - **System design/operation**
  - **Status and Future**
- **GNSS Failure Modes and Vulnerabilitites**
- **Conclusions & References**

Time and Frequency Needs Signals!

- Signals are Physical
  - Accuracy and stability are no better than the physical layer
  - Data layers disrupt the T & F signals
  - Interference to the physical signal blocks access to T & F

- Time accuracy requires access to UTC through a national lab – GNSS used
- GNSS signals are vulnerable!
- Frequency Accuracy requires access to the Cs. Atomic transition

Sync Sources: GNSS and Atomic Clocks

- **Intro: Time and Frequency Signals**
- **GNSS**
  - **System design/operation**
  - **Status and Future**

- **GNSS Failure Modes and Vulnerabilitites**

- **Conclusions & References**

The Family of Global Navigation Systems

•GPS	•Galileo	•GLONASS	•Beidou/Compass
•US	•EU	•Russia	•China
•(24+, Now 30)	•(27, 3? Now)	•(24, 27 Now)	•(35, 9 Now)

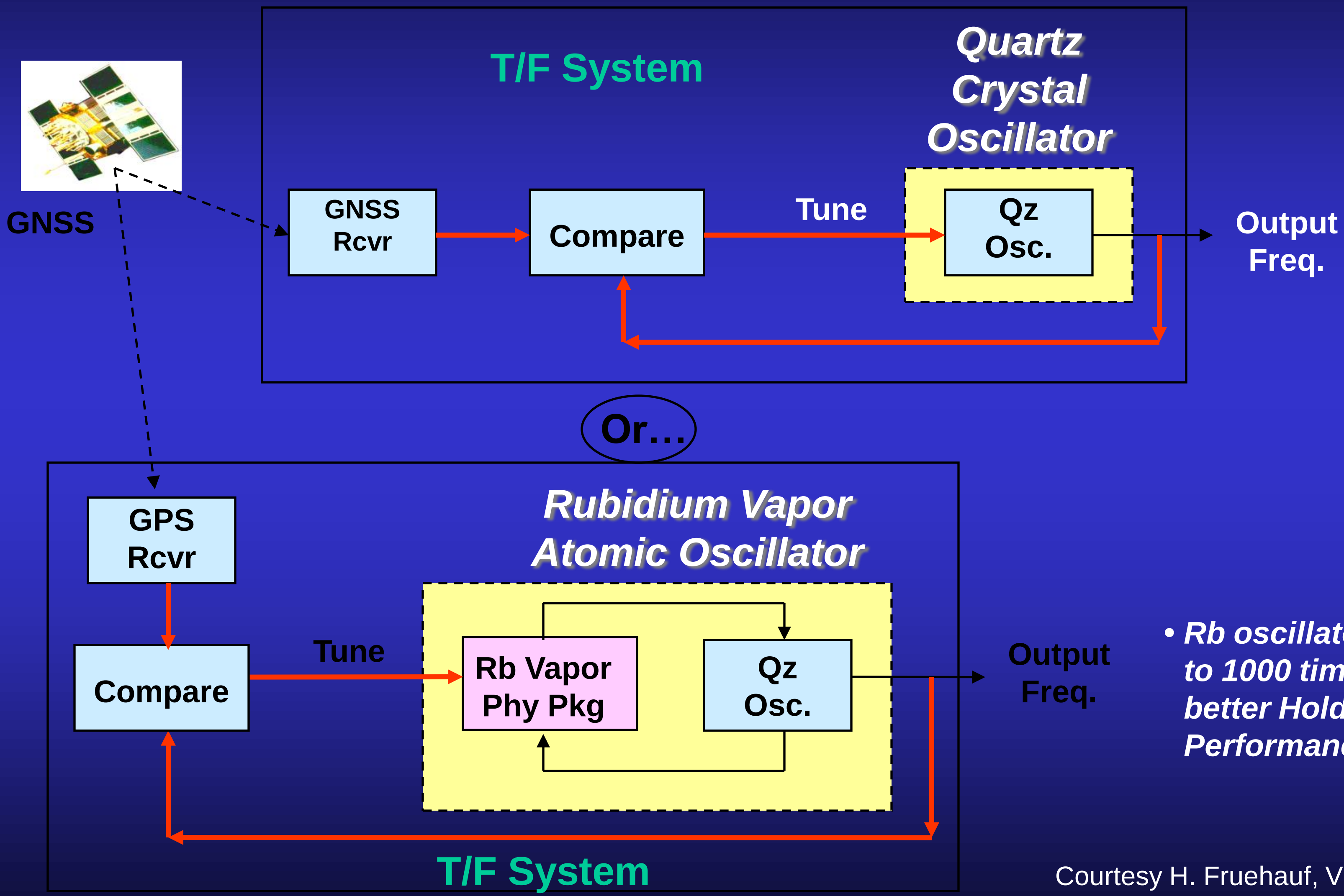
GNSS Systems: General Properties

- Position, Navigation, Timing (PNT)
- Four + synchronized timing signals from known locations in space required for navigation
- Two + frequencies measure ionosphere
- Control, Space, User Segments
- Open and Restricted Services

GNSS Systems: General Properties

- All signals are weak
  - E.g. GPS is ~-160dBm
  - All are deliberately well below the noise until the process gain
- Signals are clustered in the spectrum
- Hence it is relatively easy to jam GNSS and becoming easy to spoof

GNSS-aided Time and Frequency Systems



- ***Rb oscillator 100 to 1000 times better Holdover Performance***

Courtesy H. Fruehauf, ViaLogy LLC

Sync Sources: GNSS and Atomic Clocks

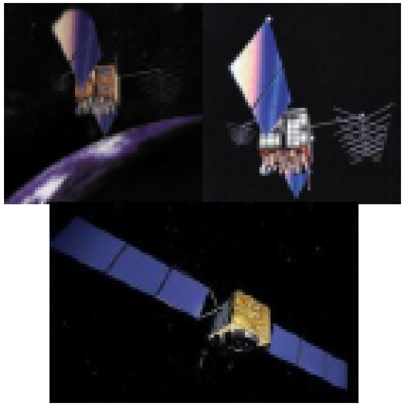
- **Intro: Time and Frequency Signals**
- **GNSS**
  - **System design/operation**
  - **Status and Future**

- **GNSS Failure Modes and Vulnerabilitites**

- **Conclusions & References**

GPS Constellation

- **Very robust constellation**
  - 30 space vehicles currently in operation
    - 10 GPS IIA, 12 GPS IIR, 7 GPS IIR-M, 1 GPS IIF
  - 4 additional satellites in residual status
  - 1 IIF satellite in test/checkout
- **Extensive International and Civil Cooperation**
  - Agreements with 53 international customers
  - 1+ billion civil/commercial users
  - Countless applications…and growing
- **Global GPS civil service performance commitment met continuously since Dec 1993**



GPS Modernization – New Civil Signals

- **Second civil signal "L2C"**
  - Designed to meet commercial needs
  - Available since 2005 without data message
  - Phased roll-out of CNAV message
  - Full capability: 24 satellites and full CNAV ~2016*

- **Third civil signal "L5"**
  - Designed to meet transportation safety-of-life requirements
  - Uses Aeronautical Radio Navigation Service band
  - 24 satellites and full CNAV ~2020*

- **Fourth civil signal "L1C"**
  - Designed for GNSS interoperability
  - Specification developed in cooperation with industry
  - Launches with GPS III in 2014
  - Available on 24 SVs ~ 2026*
  - Improved tracking performance

Urban Canyons

Improved performance in challenged environments

* FOC dates are based on our best estimate of launch schedule

2011 09 21 GPS Program Update to CGSIC – FINAL4 (3)

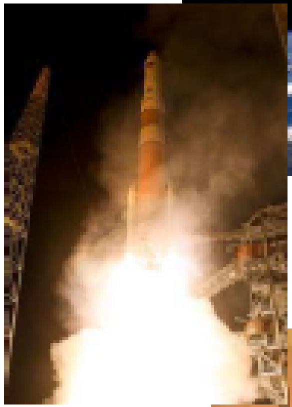
GPS IIF Status

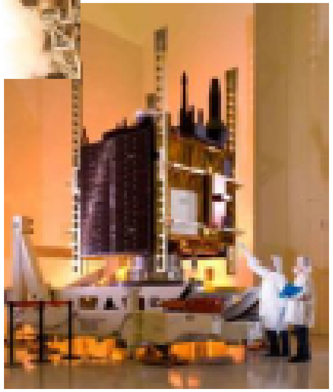
- **Launched GPS IIF-2 on 15 Jul 11**
  - SVN 63, PRN 1
  - Check out phase complete
  - Second operational L5
  - Increases the enhanced GPS clock performance coverage

- **Excellent on-orbit performance**
  - SIS URE of .30 meters (1 yr performance Jul 11)

- **10 more IIFs in the pipeline**
  - SVs 3-6 are in production

- **IIF-3 Initial Launch Capability in Feb 12**





GPS III Status

- **Newest block of GPS satellites**
  - First satellite to broadcast common L1C signal
  - Multiple civil and military signals; L1 C/A, L1 P(Y), L1M, L1C, L2C, L2 P(Y), L2M, L5
  - Three Rubidium clocks
- **Completed Critical Design Review**
- **Completed Independent Program Assessment (Milestone C)**
- **Prototype and engineering unit build/test underway**
  - Completed 54 of 59 Manufacturing Readiness Reviews
  - Completed 32 of 59 Test Readiness Reviews
- **GPS Nonflight Satellite Testbed (GNST) started 1 month early**
- **Manufacturing Readiness Review initiated**
- **Completed System Design Review and initiated Capability Insertion Program for SV-9+**

GLONASS Modernization Plan

1982	2003	2011	2013-2014
"Glonass"	"Glonass-M"	"Glonass-K1"	"Glonass-K2"

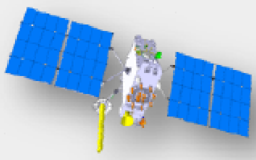
"Glonass" (1982)

- 3 year design life
- Clock stability - $5*10^{-13}$
- Signals: L1SF, L2SF, L1OF, (FDMA)
- Totally launched 81 satellites
- Real operational life time 4.5 years

"Glonass-M" (2003)

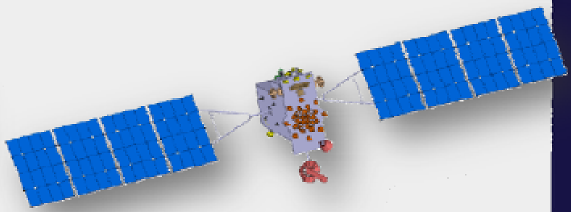
- 7 year design life
- Clock stability $1*10^{-13}$
- Signals: Glonass + L2OF (FDMA)
- Totally launched 28 satellites and going to launch 8 satellite by the end 2012

"Glonass-K1" (2011)



- 10 year design life
- Unpressurized
- Expected clock stability $\sim 10 \ldots 5*10^{-14}$
- Signals: Glonass-M + L3OC (CDMA) – test
- SAR

"Glonass-K2" (2013-2014)



- 10 year design life
- Unpressurized
- Expected clock stability $\sim 5 \ldots 1*10^{-14}$
- Signals: Glonass-M + L1OC, L3OC, L1SC, L2SC (CDMA)
- SAR

CDMA signals general structure already designed

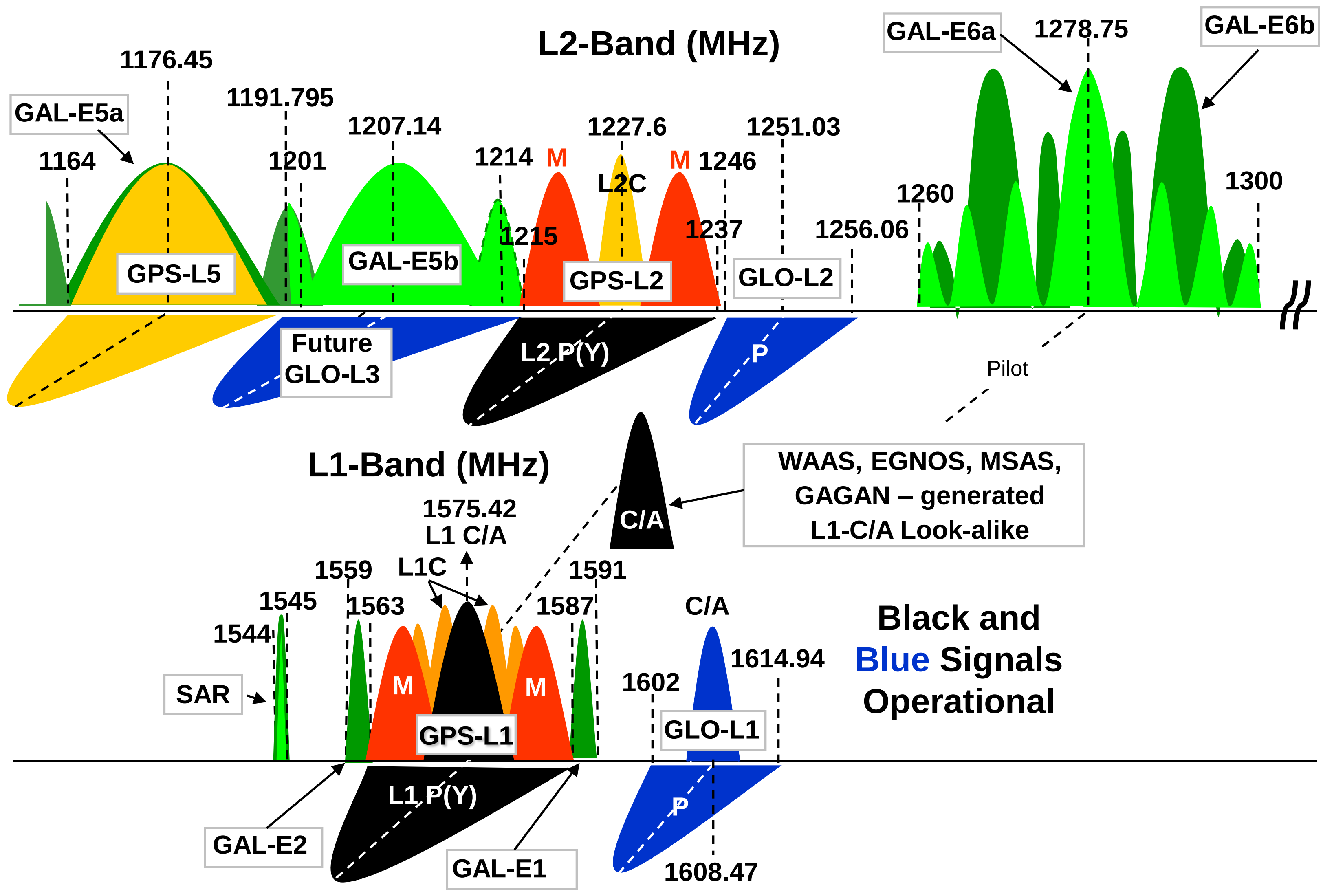
11

Presented by
Ekaterina Oleynik, Sergey Revnivykh, Central Research Institute of Machine Building
Civil GPS Service Interface Committee, Portland, Oregon, 19th September 2011

Compass Satellites as of April 2011

Date	Satellite	Orbit	Usable	System
10/31/2000	BeiDou-1A	GEO 59°E	?	BeiDou-1
12/21/2000	BeiDou-1B	GEO 80°E	Yes	
5/25/2003	BeiDou-1C	GEO 110.5°E	Yes	
2/3/2007	BeiDou-1D	supersync orbit	No	
4/14/2007	Compass-M1	MEO ~21,500 km	Testing only	BeiDou-2 (Compass)
4/15/2009	Compass-G2	Drifting	No	
1/17/2010	Compass-G1	GEO 144.5°E	Yes	
6/2/2010	Compass-G3	GEO 84°E	Yes	
8/1/2010	Compass-IGSO1	118°E incl 55°	Yes	
11/1/2010	Compass-G4	GEO 160°E	Yes	
12/18/2010	Compass-IGSO2	118°E incl 55°	Yes	
04/10/2011	Compass-IGSO3	118°E incl 55°, 200~35,991km	Yes	
2011-07-26	Compass-IGSO4	35698 x 35871 km incl 55.2 deg long: 78 to 110 deg E		

Present & Upcoming GPS, Glonass & Galileo Signals



Sync Sources: GNSS and Atomic Clocks

- **Intro: Time and Frequency Signals**
- **GNSS**
  - **System design/operation**
  - **Status and Future**
- **GNSS Failure Modes and Vulnerabilitites**
- **Conclusions & References**

Failure Modes

- GPS (GNSS) best feature and worst problem: it is extremely reliable
- Satellite failure modes can produce signals with large errors
  - Receiver Autonomous Integrity Monitoring (RAIM) should compare all satellite signals and discard errors
  - System design should compare GPS-based clock to local signals
- Receiver problems
  - Satellites set unhealthy should not be used
  - Firmware errors and wrong interpretations of specs
    - Ionosphere/troposphere models
    - Leap seconds
- Jamming: intentional and unintentional

GPS System Vulnerabilities

- Unintentional Interference
  - Radio Frequency Interference (RFI)
  - GPS Testing
  - Ionospheric; Solar Max
  - Spectrum Congestion -- LightSquared

- Intentional Interference
  - Jamming
  - Spoofing – Counterfeit Signals
  - System Damage

- Human Factors
  - User Equipment & GPS SV Design Errors
  - Over-Reliance
  - Lack of Knowledge/Training

•1 Watt
•Jammer

Factors Impacting GPS Vulnerability

- Very Low Signal Power
- Single Civil Frequency
  - Known Signal Structure
- Spectrum Competition
- Worldwide Military Applications Drive a GPS Disruption Industry
  - Jamming Techniques are Well Known
  - Devices Available, or Can be Built Easily
  - Desire for "Personal Privacy" devices

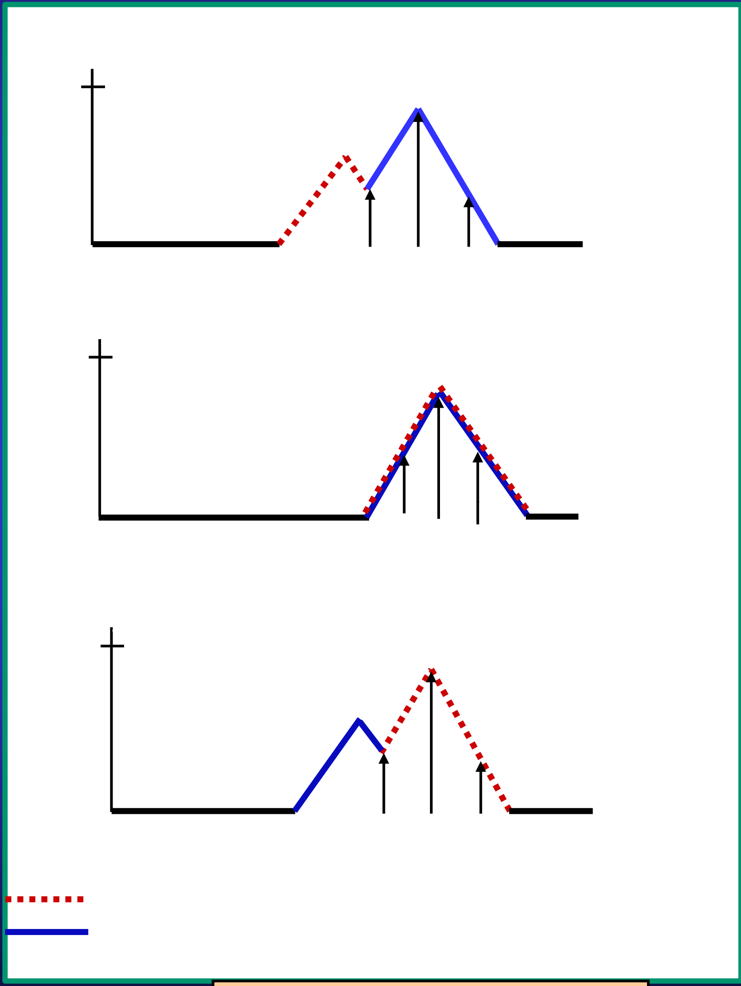
Disruption Mechanisms – Jamming

- Jamming Power Required at GPS Antenna
  - On order of a Picowatt (10^{-12} watt)
- Many Jammer Models Exist
  - Watt to MWatt Output – Worldwide Militaries
  - Lower Power (<100 watts); “Hams” Can Make
- Jamming Signal Types
  - Narrowband
  - Broadband
  - Spread Spectrum - PRN Modulation

Russian Jammer

Disruption Mechanisms - Spoofing/Meaconing

- Spoof – Counterfeit GPS Signal
  - C/A Code Short and Well Known
  - Widely Available Signal Generators
- Meaconing – Delay & Rebroadcast
- Possible Effects
  - Long Range Jamming
  - Injection of Misleading PVT Information
- No “Off-the-Shelf” Mitigation



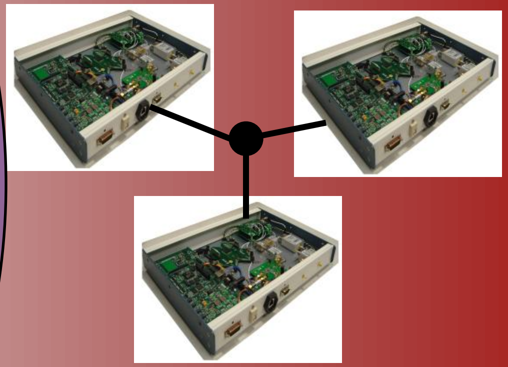
•Successful Spoof

Civil GPS Spoofing Threat Continuum*

Simplistic | *Intermediate* | *Sophisticated*

Commercial signal simulator

Portable software radio



Coordinated attack by multiple phase-locked spoofers

- *** Courtesy of Coherent Navigation, Inc**

GPS Spoofing Detection / Mitigation

- Civilian GPS signals are without authentication or encryption, making detection and mitigation more difficult
- Most mitigations involve integrity checking via multiple clocks, user-supplied position, and RF signal anomalies
- Recommend vendors add integrity checking to time/frequency servers
- Receivers should detect signal anomalies such as
  - Wrong time (compared to reference clock)
  - Suspiciously low noise
  - Excessive signal strength
  - Artificial spacing of signals
  - Limited short term jitter or variation in signal strength
  - All satellites have the same signal strength
  - High level sanity checks (e.g., no large position discontinuities)

Sync Sources: GNSS and Atomic Clocks

- **Intro: PRS and Time vs Frequency**
- **GNSS**
  - **System design/operation**
  - **Status and Future**
  - **Failure Modes**
- **Atomic Clocks**
- **Conclusions & References**

Conclusions

- GNSS Now
  - Global GPS civil service performance commitment met/exceeded continuously since Dec 93
  - Glonass operational, committed to replenish
  - Galileo, Compass with new satellites
  - Augmentation systems exist
- GNSS Future
  - GPS: new signals, more accuracy, yet backward compatible, more integrity information
  - New/other systems: Glonass, Galileo, Compass, QZSS
  - New services: LBS, ITS
- GPS/GNSS vulnerabilities
  - GNSS must not be over-relied upon
  - Receiver systems should detect anomalies

- Many resources are available

GNSS Resources

- U.S. Coast Guard Navigation Information Center
  - Voice Announcement ++1-703-313-5907
  - Resource Person ++1-703-313-5900
  - Web Page http://www.navcen.uscg.gov/
  - Civil GPS Service Interface Committee (CGSIC) – GNSS status and other info: http://www.navcen.uscg.gov/cgsic/meetings/48thMeeting/48th_CGSIC_agenda_final.htm
- U.S. Space-Based Positioning, Navigation, and Timing Policy: http://pnt.gov/policy/
- International GNSS Service (IGS)
  - http://igscb.jpl.nasa.gov/
- US Timing Labs
  - NIST info: http://www.boulder.nist.gov/timefreq/index.html
  - U.S. Naval Observatory: http://tycho.usno.navy.mil/gpstt.html
- GPS World: www.gpsworld.com
- Inside GNSS: www.insidegnss.com
- Institute of Navigation www.ion.org

Extra Slides

GNSS for Telecom Timing

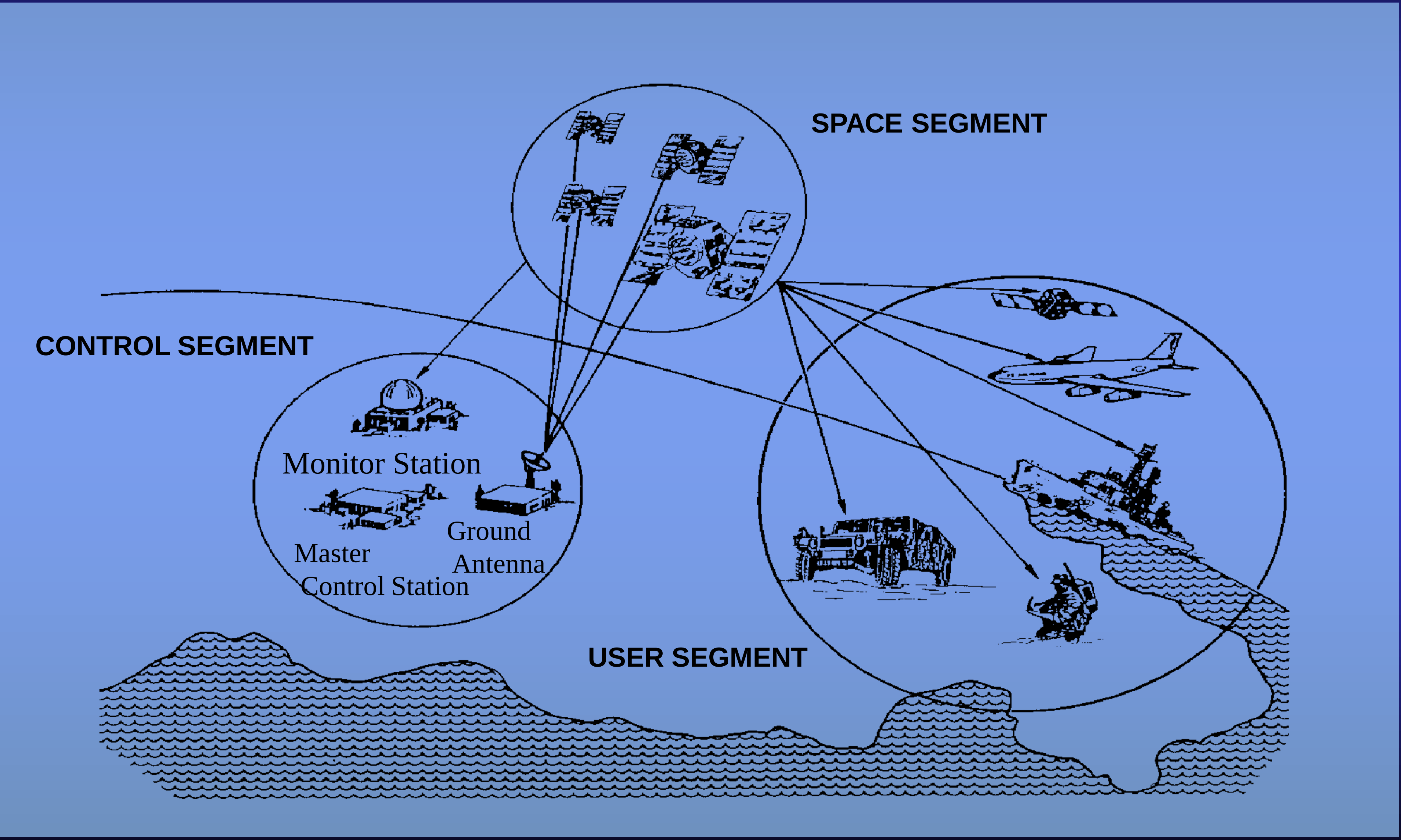
- Antenna required
  - Top of building implies space rental, lightning issues
  - Through window gives limited visibility, sats come and go, GEOs are fixed
- Receiver needs Qu or Rb oscillator
  - Provides signal, steered to sats
  - Stability/cost trade-offs
- Telecom timing signals required
- Error/failure/attack mitigation
  - RAIM
  - Duplicate/backup timing

Upcoming Systems Integrating Communications and Navigation

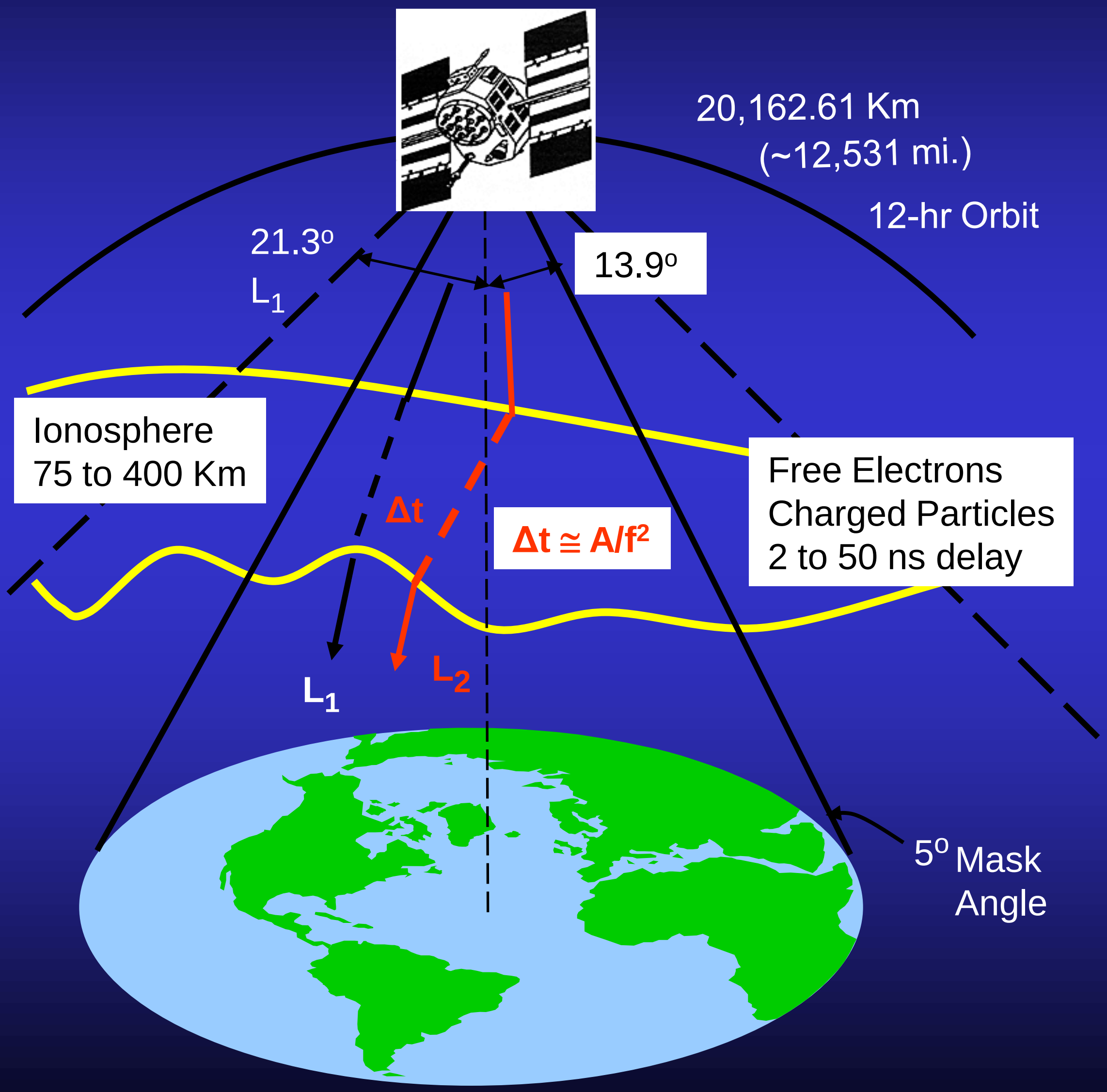
- Location Based Services
  - Social Networking
  - Advertising
  - Emergency services

- Intelligent Transportation System
  - Provide road and traffic conditions to users
  - Send user’s conditions to management systems

GPS (GNSS) System Configuration - Three Major Segments



GPS Satellite Signals



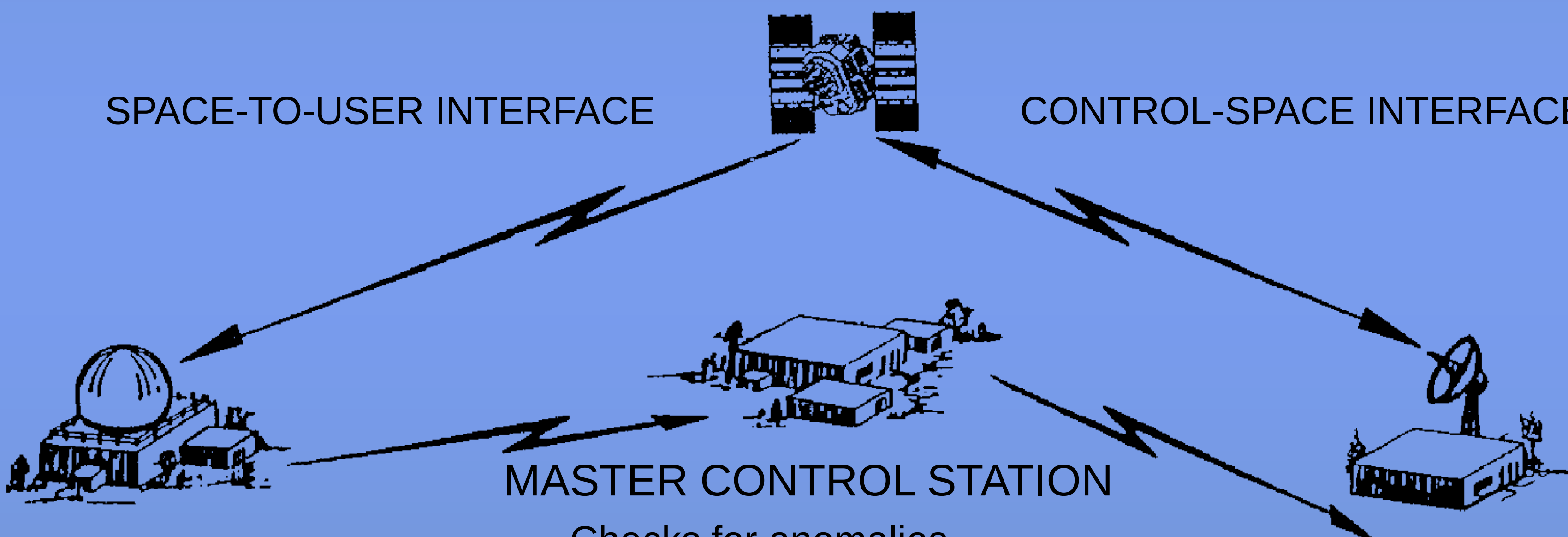
- L_1 **1575.42 MHz**
  C/A-Code 1.023 Mcps,
  P-Code 10.23 Mcps
  Data 50 bps
- L_2 **1227.6 MHz**
  P-Code 10.23 Mcps
  Data 50 bps
- **Four Satellites needed for 3-D navigation**
- **Maximum Doppler Shift between Satellites ~ ± 6KHz**

Courtesy H. Fruehauf, ViaLogy LLC

Control Segment

SPACE VEHICLE (SV)

Broadcasts the SIS PRN codes, L-band carriers, and 50 Hz navigation message stored in memory



MASTER CONTROL STATION

- Checks for anomalies
- Computes SIS portion of URE
- Generates new orbit and clock predictions
- Builds new upload and sends to GA

MONITOR STATION

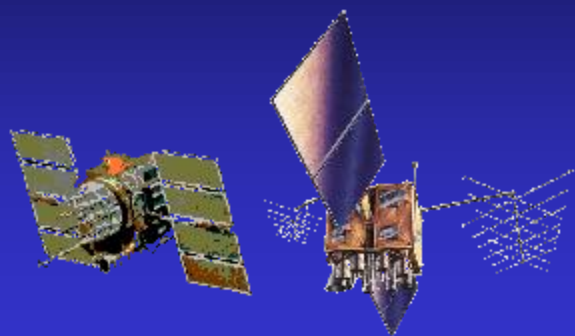
- Sends raw observations to MCS

GROUND ANTENNA

- Sends new upload to SV

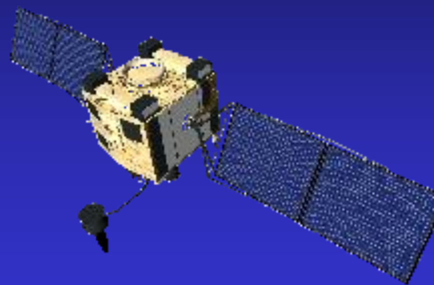
GPS Modernization Plan

Block IIA/IIR

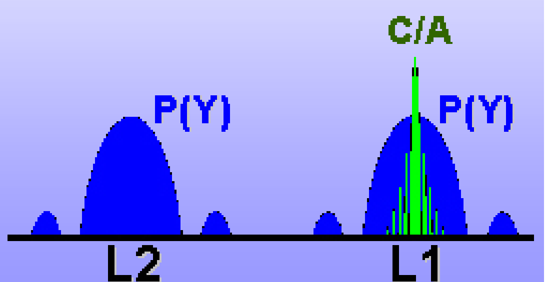


Block IIR-M, IIF

Block III



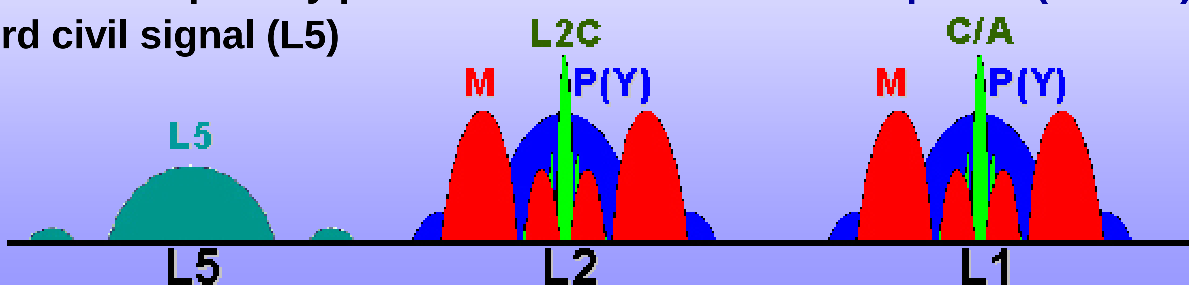
<u>IIA / IIR</u>: Basic GPS
- **C/A civil signal (L1C/A)**
- **Std Service, 16-24m SEP**
- **Precise Service, 16m SEP**
  - **L1 & L2 P(Y) nav**



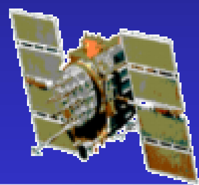
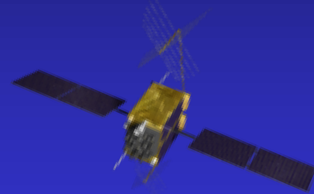
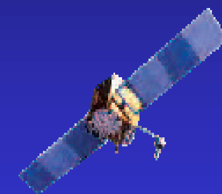
<u>IIR-M</u>: IIA/IIR capabilities &
- **2nd civil signal (L2C)**
- **New military code**
- **Flex A/J power (+7dB)**

<u>IIF</u>: IIR-M capability plus
- **3rd civil signal (L5)**

<u>III</u>: IIF capabilities &
- **Improved civil signal (L1C)**
- **Increased accuracy (4.8-1.2m)**
- **Evaluating integrity improvements**
- **Navigation surety**
  - **Increased A/J power (+20 dB)**



GPS Modernization Programs

	1995	2005	2010	2014 - 2025
	GPS IIA/GPS IIR	GPS IIR-M	GPS IIF	GPS III
Space Segment				
	• Standard Positioning Service (SPS) ○ Single frequency (L1) coarse acquisition code navigation • Precise Positioning Service (PPS) ○ Y-Code (L1 P(Y) & L2 P(Y))	• IIA/IIR capabilities plus: ○ 2nd civil signal (L2C) ○ M-Code (L1M & L2M)	• IIR-M capability plus ○ 3rd civil signal (L5) ○ 12 year design life	• Backward compatible • 4th civil signal (L1C) • Increased accuracy • Increased integrity • Increased design life

Ground Control Segment	Legacy Control System	Architecture Evolution Plan (AEP)	Next Generation Control Segment (OCX)

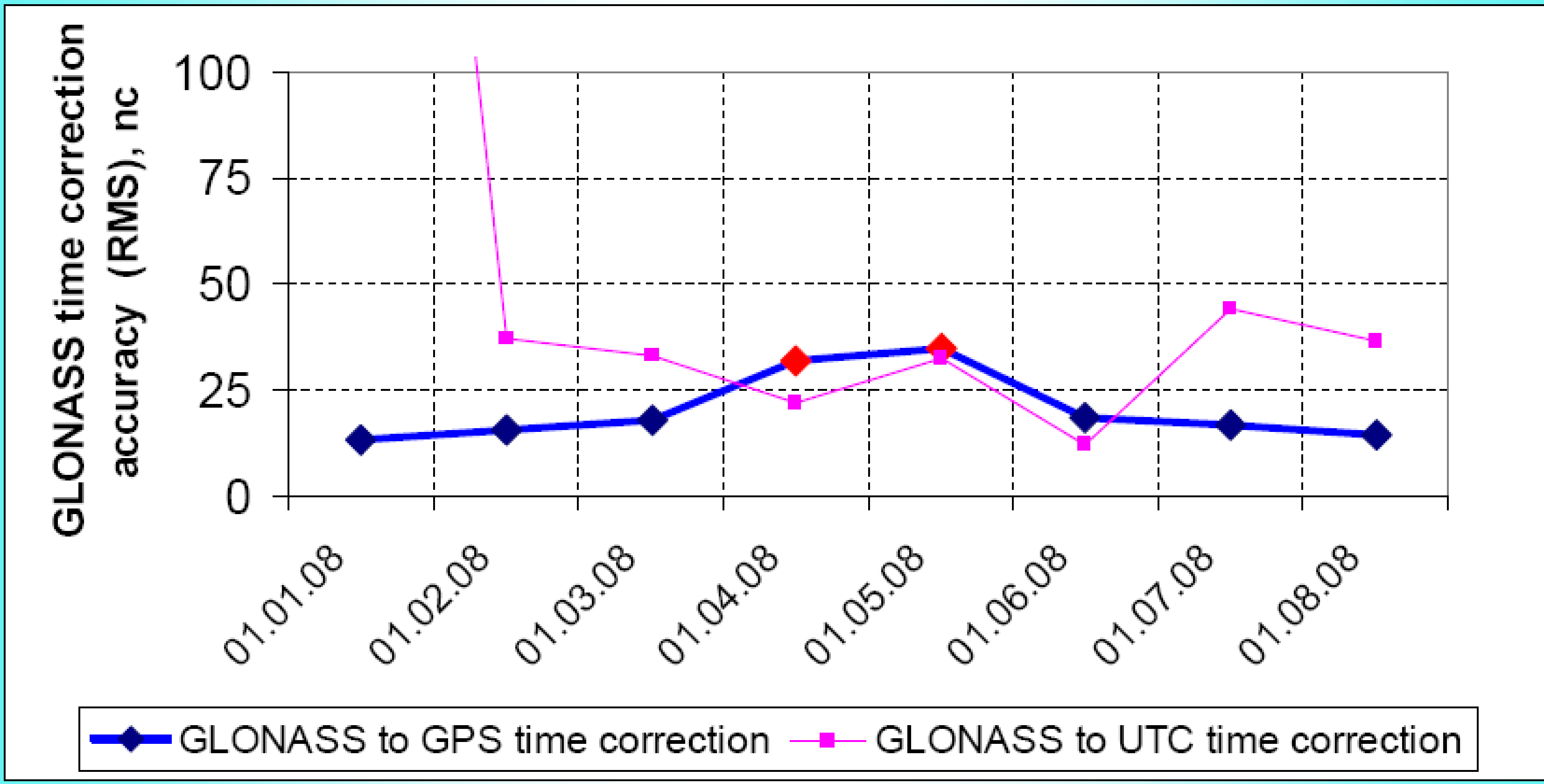
•Courtesy Thomas D. Powell, GPS Systems Engineering, The Aerospace Corporation, 18 April 2010

GPS III

- Concept Definition completed in 2005
- Contract issued 2008
- GPS-III (2013 ? -): New features are being considered to increase reliability and accuracy
  - Faster time to alert or correct failures (integrity)
  - More accuracy
  - More availability
  - Increased signal strength

GLONASS

GLONASS TIME



•Presented by Reshtec Co., ICG, 30July2009

GLONASS

РОСКОСМОС

Navigation satellite "Glonass-M"

РЕШЕТНЕВ

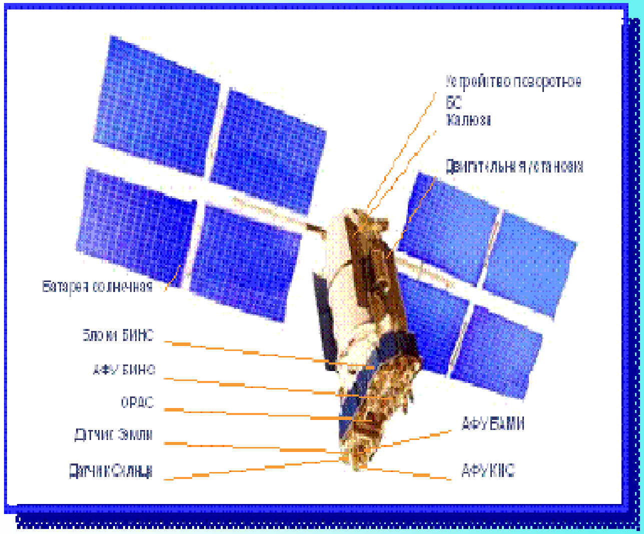
Main features

- Guaranteed life time — 7 years;
- Mass — 1415 kg;
- Clock stability — 1e-13;
- Attitude control accuracy — 0,5 deg;
- Level of unpropogated forces — 5e-11 m/c^2
- Navigations signals:

4 signals in L1 and L2 bands with FDMA

Main features

- Extended life time
- Second civil signal L2
- Increased board clock stability
- Improved attitude and the solar panel pointing accuracy
- Improved dynamic model
- Using Inter Satellite Link (ISL) measurements for improvement ephemeris and clock navigation data



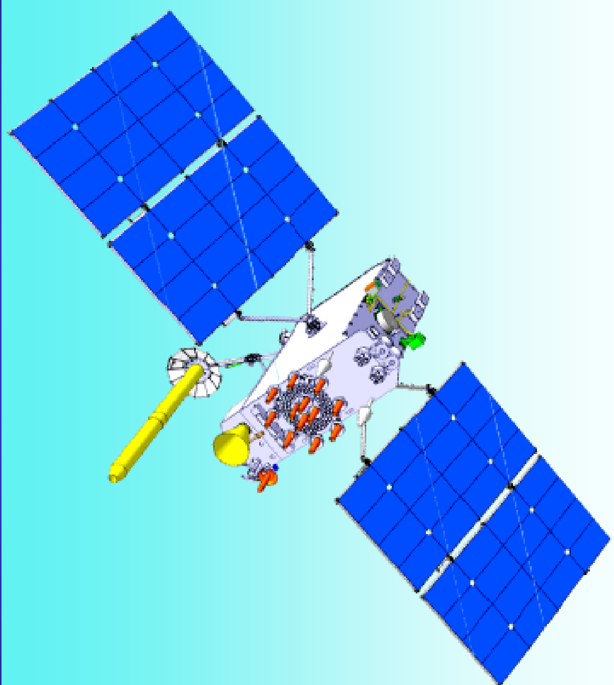
• Presented by Reshtec Co., ICG, 30July2009

GLONASS

РОСКОСМОС

Navigation satellite “Glonass-K”

РЕШЕТНЕВ



Main features	
Guaranteed life time	10 years;
Mass	995 kg;
Clock stability	1e-14;
Level of unpropogated forces	1e-11 m/c2
Navigations signals:	
Four FDMA signals in L1 and L2 bands	
New CDMA signals in L1, L2, L3 bands	

Main features

- Extended life time;
- New CDMA navigating signals
- Improved attitude and the solar panel pointing accuracy
- Dramatically decreasing level of the unpropogated not gravity forces;
- Provides the high precision thermal control for onboard clock (0,1 ° - 0,5 ° C);
- Additional suffering disaster payload (Cospas-Sarsat)

ICG WORKSHOP 30..31 July 2009 18

•Presented by Reshtec Co., ICG, 30July2009

GLONASS

The direction of GLONASS navigation signals modernization

РОСКОСМОС

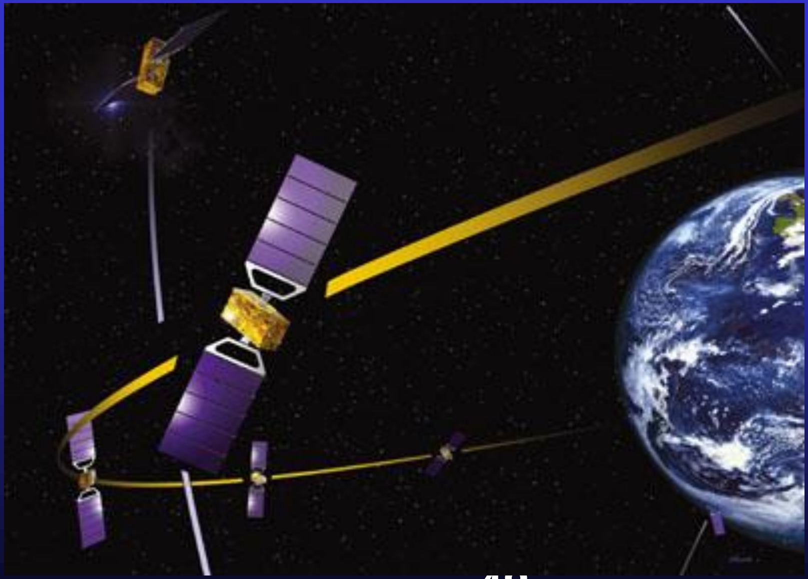
РЕШЕТНЕВ

- Introduction of new CDMA signals
- Provide better potential accuracy for pseudorange and phase measurements
- Provide a better interference and multipath resistance of GLONASS signals
- Provide of greater interoperability with GPS and future GALILEO and other GNSS

•Presented by Reshtec Co., ICG, 30July2009

GALILEO

- Galileo will be Europe’s own global navigation satellite system
- It will be interoperable with GPS and GLONASS, the two other global satellite navigation systems.
- Galileo is a joint initiative of the European Commission (EC) and the European Space Agency (ESA).
- Consists of 30 medium Earth orbit satellites, associated ground infrastructure, and regional/local augmentations.
- Will offer a basic service for free (Open Service), but will charge user fees for premium services.



The GALILEO Satellite Services

Position, Velocity and Time Services:

- **Open Service** - providing positioning, navigation and timing services, free of charge, for mass market navigation applications (future GPS SPS)
- **Commercial Service** - provides added value over the Open Service providing commercial revenue, such as dissemination of encrypted navigation related data (1 KBPS), ranging and timing for professional use - with service guarantees
- **Safety of Life Service** - Comparable with “Approach with Vertical Guidance” (APV-II) as defined in the ICAO Standards and Recommended practices (SARPs), and includes Integrity
- **Public Regulated Service** - for applications devoted to European/National security, regulated or critical applications and activities of strategic importance - Robust signal, under Member States control

Support to Search and Rescue

- Search and Rescue Service coordinated with COSPAS SARSAT

Compass/ Beidou

- China may complete a 12-satellite regional system by 2012
  - 5 in Geostationary orbits
  - 3 in Inclined Geostationary orbits
  - 4 in Middle-earth orbits
- China is currently developing COMPASS to reach Full Operational Capacity (FOC) around 2020
  - 24 MEOs
  - 3 GEOs (including 2 Beidou-1 satellites)
  - 3 IGSOs
- A draft Interface Control Document (ICD) may be available in 2010
- http://www.insidegnss.com/node/1697

QZSS

Proposed Orbit for QZS

period : 23 hours 56 minutes
(geosynchronous)
inclination : 43±4 degrees
eccentricity : 0.075±0.015
(preference for Japan)
orbital planes : 3 (spacing 120°)
central laltitude : 135±5 deg.E

see IS-QZSS in
http://qzss.jaxa.jp/is-qzss/index_e.html

3 satellites is needed for 24 hr service.
The 1st QZS is to be launched in 2010.

footprint in one day

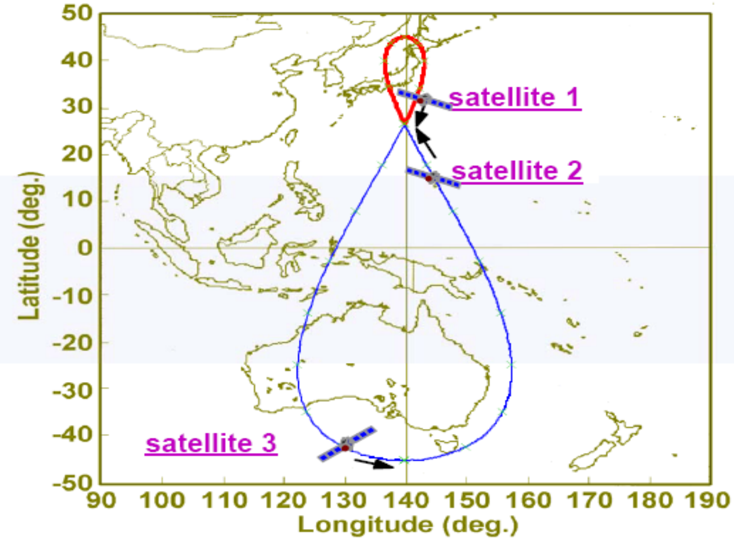


Figure “8”

• Presented by Shin’ichi Hama, et. Al., ION GNSS 2009

• 1st QZS launched Sep 11, 2010

Regional Satellite Navigation Systems

- Indian Regional Navigational Satellite System (IRNSS)
  - Autonomous regional satellite navigation system consisting of 7 satellites and ground segment
  - Developed by Indian Space Research Organization
- Quasi-Zenith Satellite System (QZSS) – Japan
  - Will provide an augmentation service which, when used in conjunction with GPS, GLONASS or Galileo, will provide enhanced navigation in the Far East
  - Consists of three satellites in highly elliptical orbits - satellites dwell at high elevations in the sky allowing enhanced coverage in urban canyons.

Satellite-Based Augmentation Systems (SBAS)

- **Wide Area Augmentation System (WAAS)**
  - Commissioned in 2003 and operated by the U.S. Federal Aviation Administration (FAA), to enable aircraft navigation in the U.S. National Airspace System (NAS)
- **European Geostationary Navigation Overlay System (EGNOS)**
  - Three geostationary satellites and a network of ground stations
  - Augments the US GPS satellite navigation system in Europe
- **Japan's Multifunction-Transport-Satellite Satellite Augmentation System (MSAS)**
  - MSAS for aviation use was commissioned in 2007
- **India's GPS and Geo-Augmented Navigation System (GAGAN) (operational in 2011)**
- **Russian System of Differential Corrections and Monitoring (SDCM) (operational in 2011)**

Other GPS Augmentations

- **Nationwide Differential GPS System (NDGPS):**
  – Ground-based augmentation system of ~80 sites operated by the U.S. Coast Guard, Federal Railroad Administration, and Federal Highway Administration, to provide increased accuracy and integrity to U.S. users on land and water.
- **Local Area Augmentation System (LAAS):**
  – Augmentation to GPS that focuses its service on the airport area (approximately a 20-30 mile radius)
  – Broadcasts correction message via a very high frequency (VHF) radio data link from a ground-based transmitter
  – LAAS is a US activity led by the FAA, but other nations are developing their own ground based augmentation system projects
- **NASA Global Differential GPS (GDGPS) System:**
  – GDGPS is a commercial high accuracy (~ 10cm) GPS augmentation system, developed by the Jet Propulsion Laboratory (JPL) to support real-time positioning, timing, and orbit determination requirements.

GNSS Interoperability Issues

- Coordinate System
  - GPS and Galileo plan on using the same system: ITRF
  - Glonass uses a slightly different system
- Time Scale
  - GPS and Galileo have agreed to transmit the GPS/Galileo Time Offset (GGTO)
  - Goal: an objective of three nanoseconds (one meter) accuracy for the GGTO message has been accepted
  - Glonass uses a different time scale, though known relationships are kept within bounds
- Signal Compatibility
  - Generally all systems can be received by the same system

GNSS Signals Are Vulnerable to Jamming

- Signals can be easily jammed
- Several incidents of accidental jamming
- Most telecom receivers can go into holdover for at least a week with few ill effects
- Wireless base-stations can be affected adversely