GPS-SAASM and Direct P(Y) Acquisition

as applied to Communications and Command/Control Terminals

Commercial Release

Hugo Fruehauf
FEI-Zyfer Inc.
July 2004
hxf@fei-zyfer.com

Discussion Outline

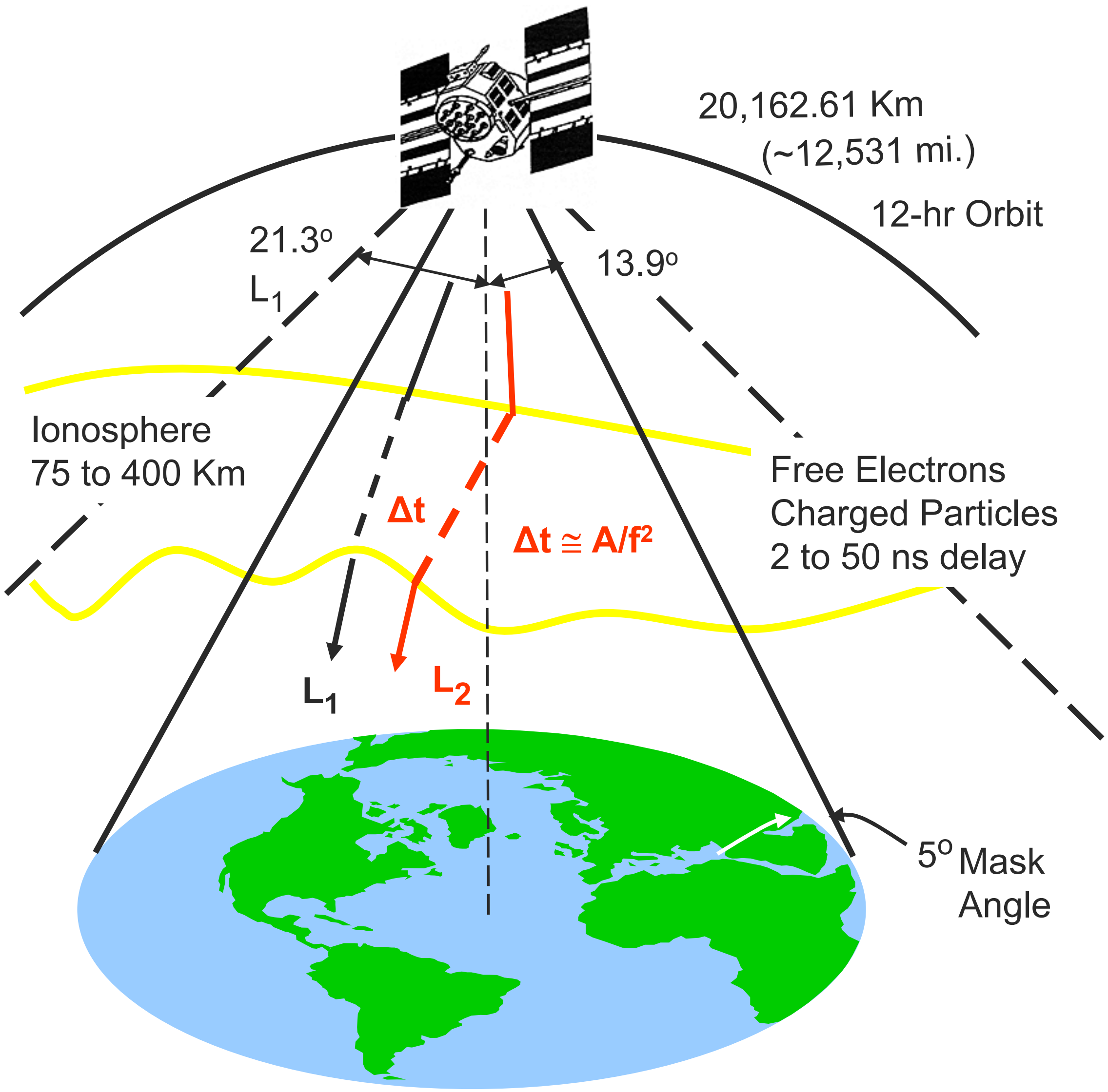
- GPS Basics
- GPS Signal Realities
- What is SAASM all About?
- Future GPS and Galileo Signals
- The GPS Sync Engine
- Important SAASM Documents
- GPS Keying Basics
- Key Ordering Details
- GPS Signal Acquisition

...Some Ground Rules

- This is the commercial release of the otherwise “For Official Use Only” (FOUO) briefing of the new-generation military GPS-SAASM infrastructure
- For a FOUO briefings, JPO requires that this be done only between PPS RCVR and HAE suppliers and authorized PPS user contractors/agencies of the U.S. and authorized Allies
- GPS-JPO interface:
  - CAPT. Erik N. Quigley SMC/CZUS – SAASM PM
    erik.quigley@LOSANGELES.AF.MIL
    (310) 363-2348 Ph., (310) 363-3844 Fax
  - COL Billy H. Welch SFAE-IEW&S-NS – Navigation Systems PM
    bh.welch@us.army.mil
    (310) 363-2922 Ph., (310) 363-0594 Fax
  - http://gps.losangeles.af.mil/index.html
  - https://www.gpsjpo.com-uesecurity

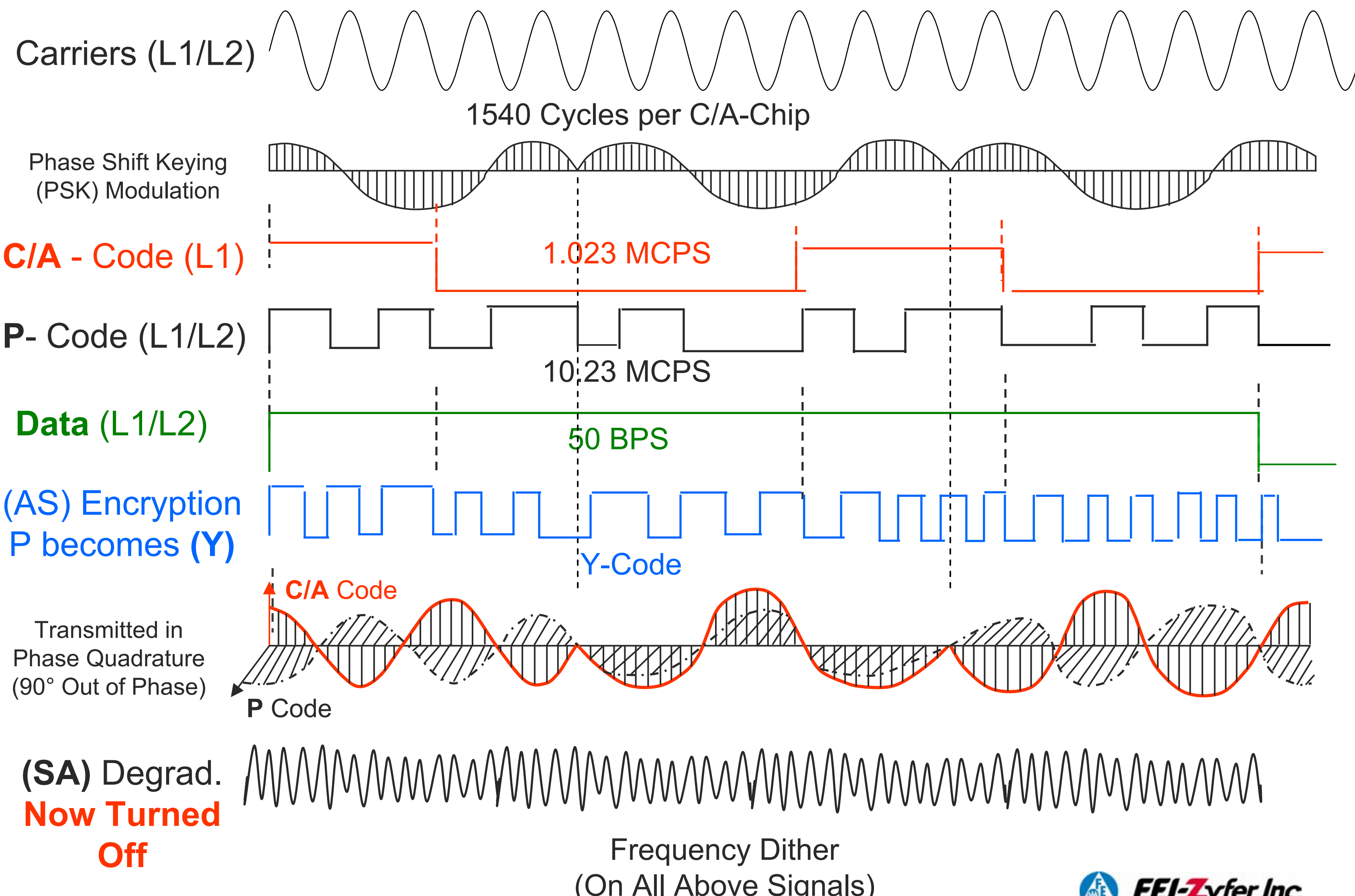
GPS Basics

GPS Satellite Signals



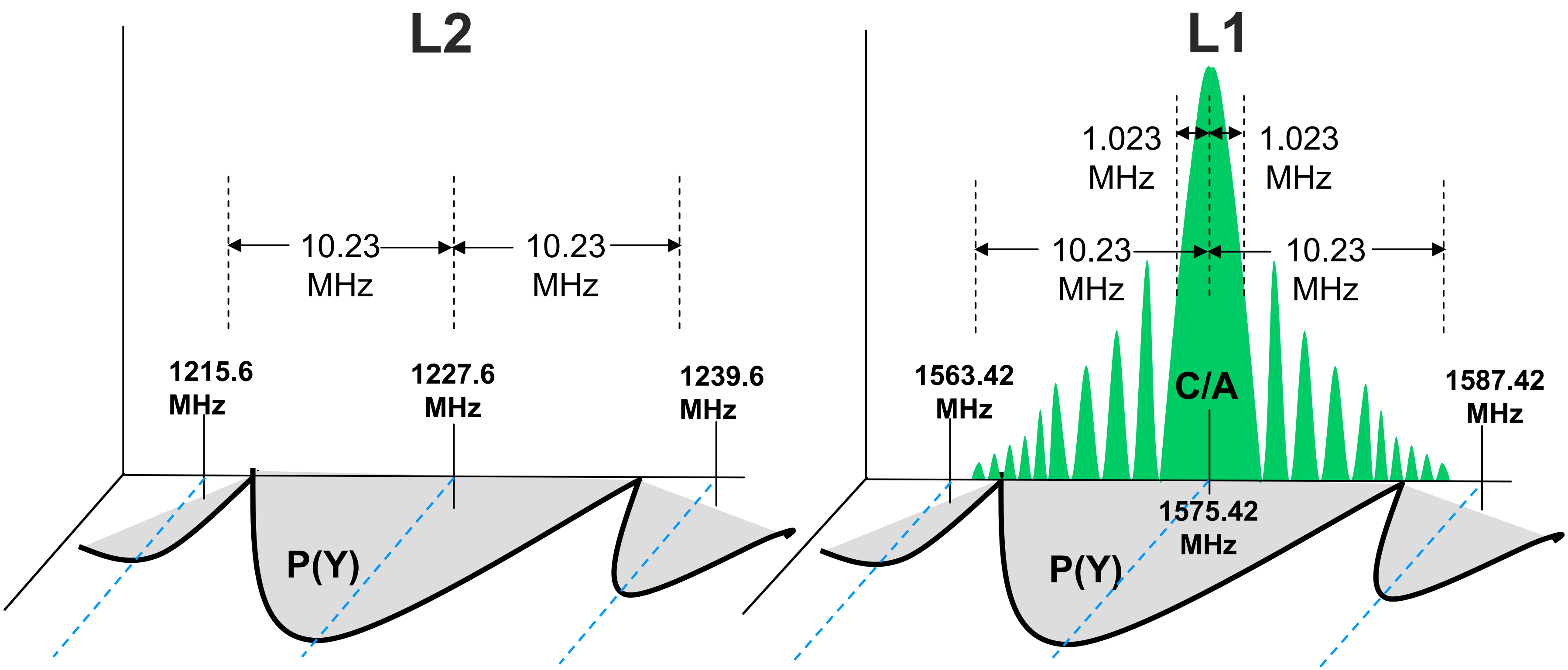
- L_1 **1575.42 MHz**
  C/A-Code 1.023 Mcps,
  P-Code 10.23 Mcps
  Data 50 bps
- L_2 **1227.6 MHz**
  P-Code 10.23 Mcps
  Data 50 bps
- **Four Satellites needed for 3-D navigation**
- **Maximum Doppler Shift between Satellites ~ ± 6KHz**

The GPS Carrier Modulation Signals



FEI-Zyfer Inc.

GPS Signal Structure



Spread Spectrum Signal, ~20dB below a receiver ambient noise level

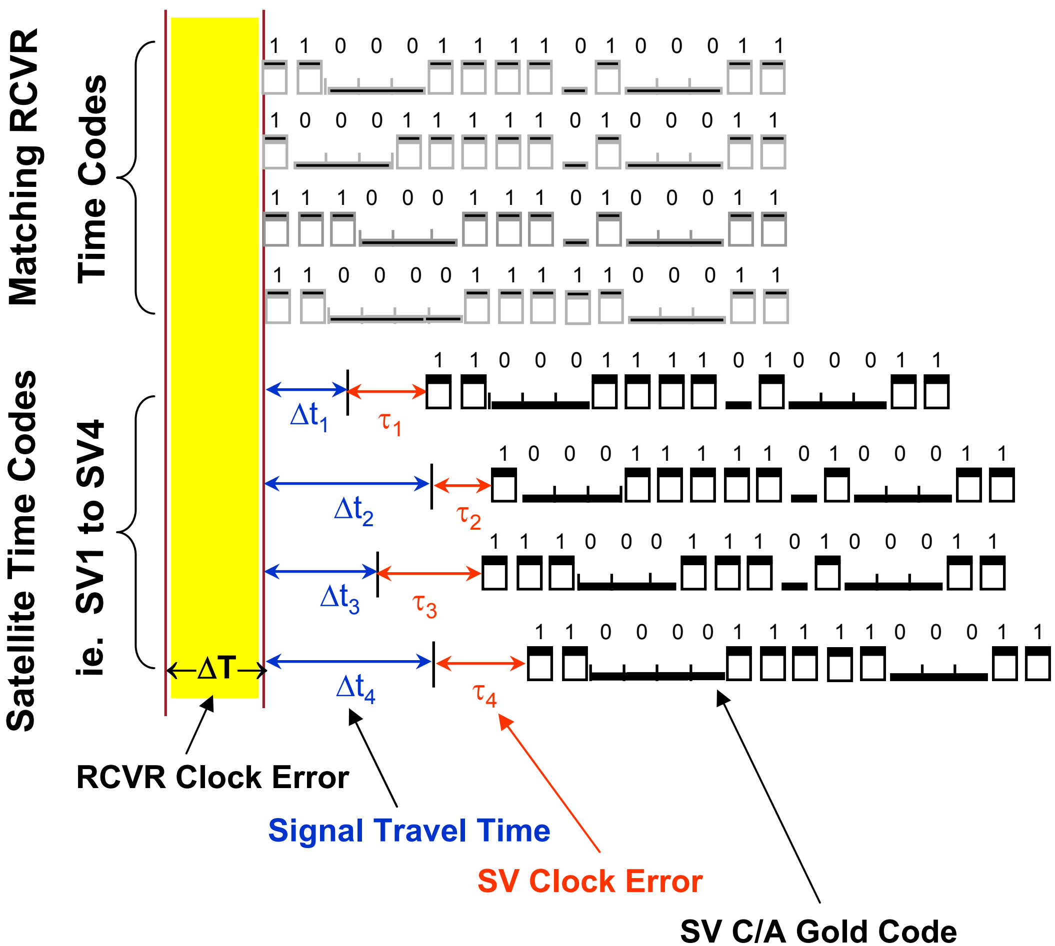
(Said to represent energy of a 25 watt light bulb at 11,000 miles distance)

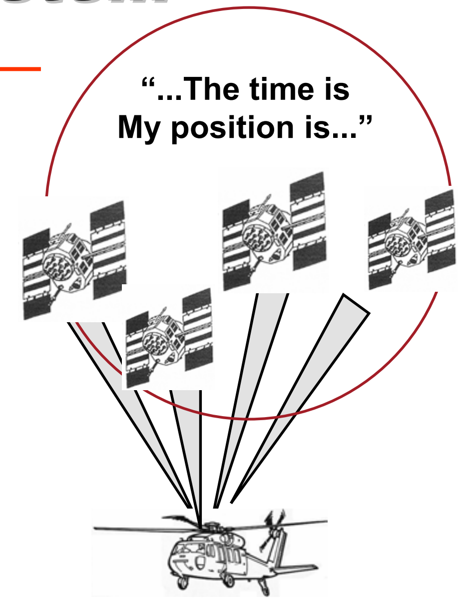
Carrier-Frequency	C/A Code	P-Code	(+) Encryption	Data	(S/A) Degradation
L1 1575.42 MHz	1.023 MHz Chipping Rate	10.23 MHz Chipping Rate	NSA/JPO Crypto Keys For Authorized Users Only	50 BPS	Selective Availability of C/A Signal
	Code Period 1023 Chips	Code Period 2.35469 x 10^{14} Chips (~38 weeks)		1500 Bit Frame, 5 subframes (30S); Each Subframe 300 Bits (6S); 30 Bits Word, 24 Bearer Bits, 6 Bits Parity; Total 12.5 Minutes	Dither at Output of Sat Clocks
	Code Repeats Every 1 ms ~1microsec Time Per Chip	Code is Reset Every Week		"How" Word For P-Code Acq. (Each Subframe)	Degradation Level of C/A Selectable by Grd. Comd.
	Different Gold Code I.D.'s Each Sat	6.19658 x 10^{12} Chips/Week		Clock and UTC Correction	**NOW Turned Off**
	Spatial Length per bit: 290 m, 960 ft.	~0.1microsec Time Per Chip		User Range Accur. (URA)	
		Same Code for Each Sat, But Different 7-day Section		Sat Health	
		37, 7-day Sections Available		Sat Configuration	
		Spatial Length per bit: 29 m, 96 ft.		Ionospheric Correction Model	
				Ephemeris	
				Coordinate Sys.	
				Almanac	
L2 1227.6 MHz	No-C/A	P-Only	Yes	Yes	Yes

GPS Signal Structure Overview

Space Borne 1-Way 3D Ranging System

The Realistic GPS System





$R_1 = C(\Delta t_1 + \Delta T - \tau_1)$

$R_2 = C(\Delta t_2 + \Delta T - \tau_2)$

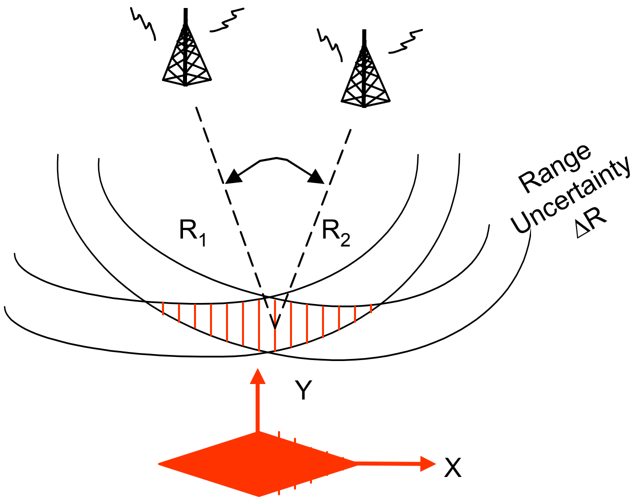
$R_3 = C(\Delta t_3 + \Delta T - \tau_3)$

$R_4 = C(\Delta t_4 + \Delta T - \tau_4)$

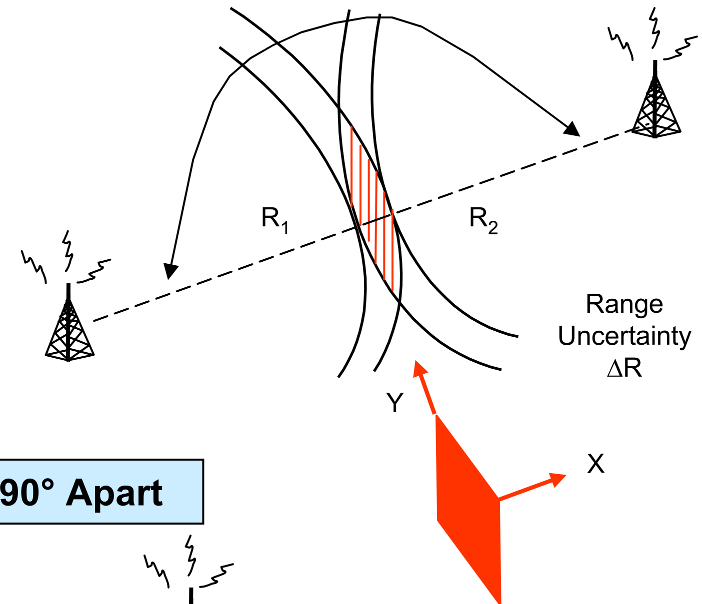
4 Equations — 4 Unknowns

What is Geometric Delusion of Precision (GDOP)?

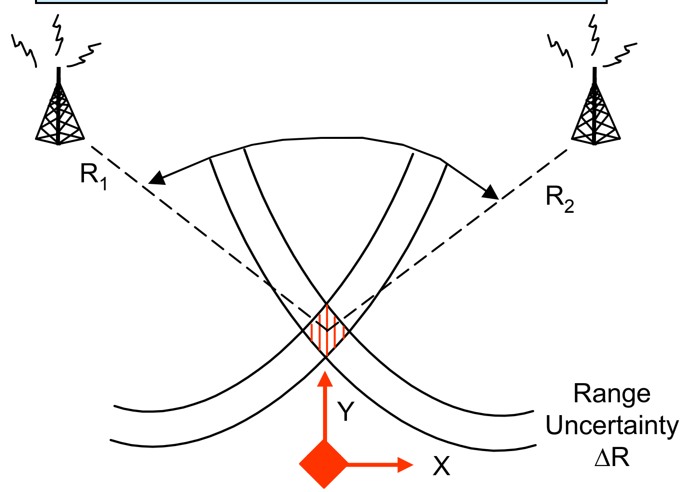
Two Transmitters Near Side by Side



Two Transmitters Near 180° Apart



Two Transmitters 90° Apart

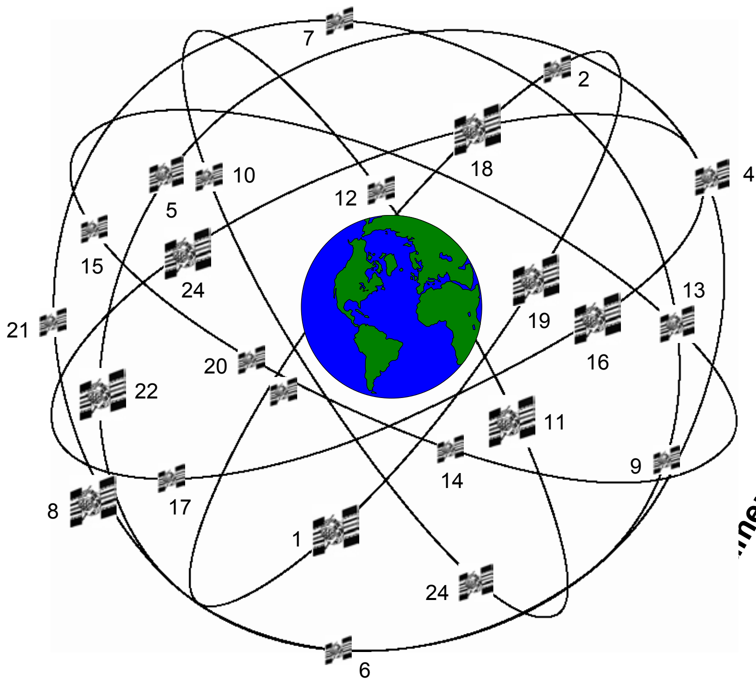


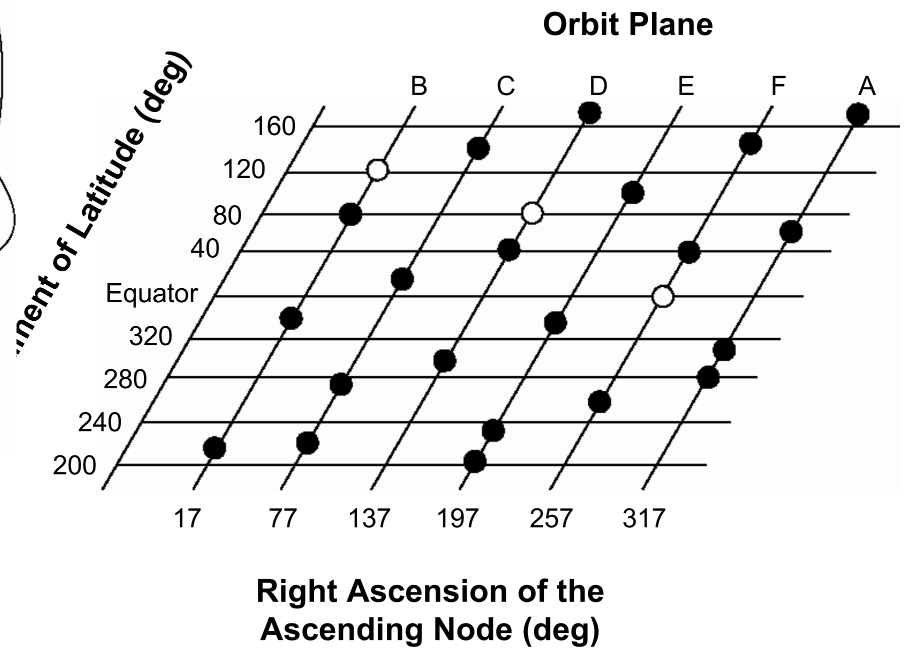
Optimum

$$\Delta X = \Delta Y$$

$$\sim \sqrt{2}(X)(\Delta R)$$

Satellite Constellation





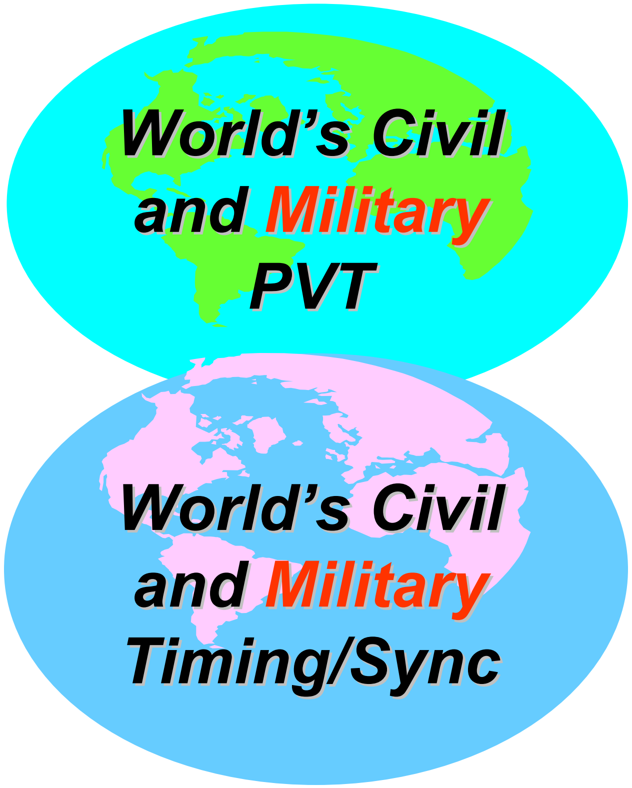
All near perfect circular orbits;
21 to 24 Satellites required for
24 x 7 coverage to Spec Accuracy

28 GPS Satellites Operating as of August 2003

FEI-Zyfer Inc.

GPS Signal Realities

The Two Worlds of GPS-SAASM

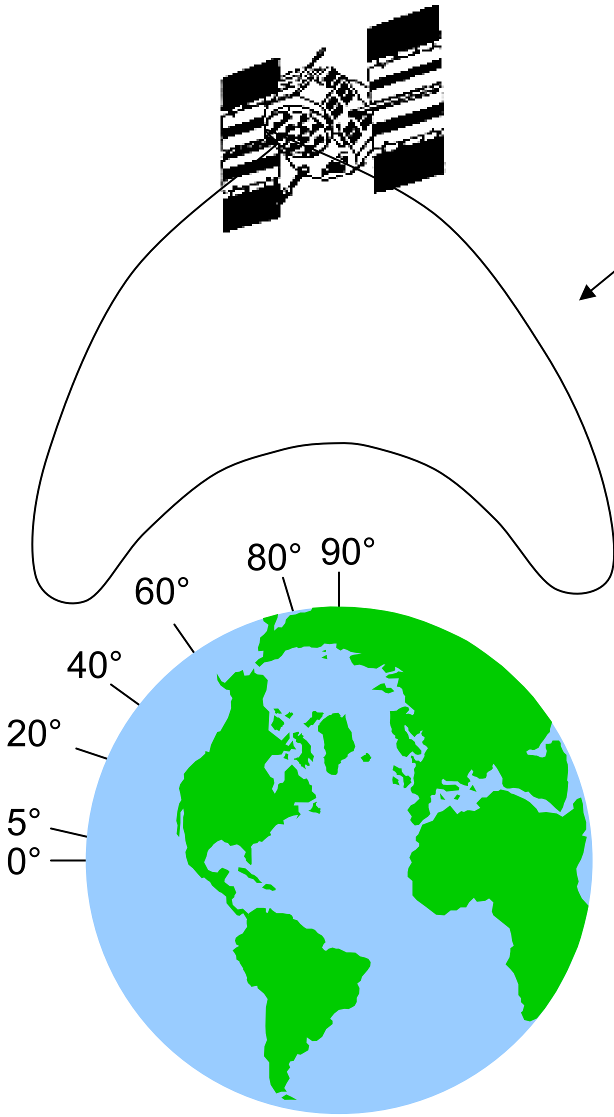


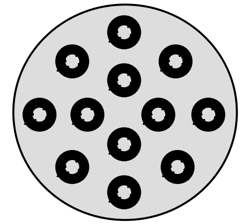
- Navigation and Positioning – PVT (Position, Velocity, and Time)

- Precision Time and Frequency Generation and Synchronization

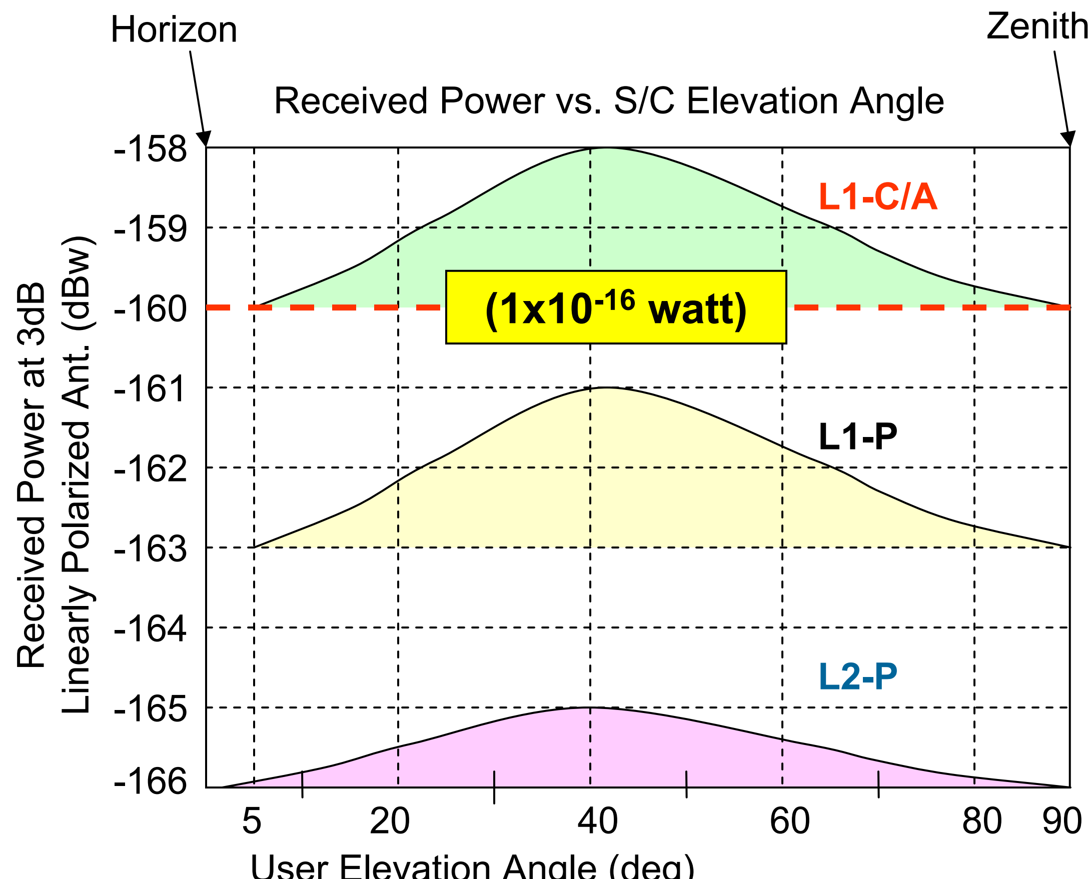
Focus of Briefing!

GPS Signal Realities

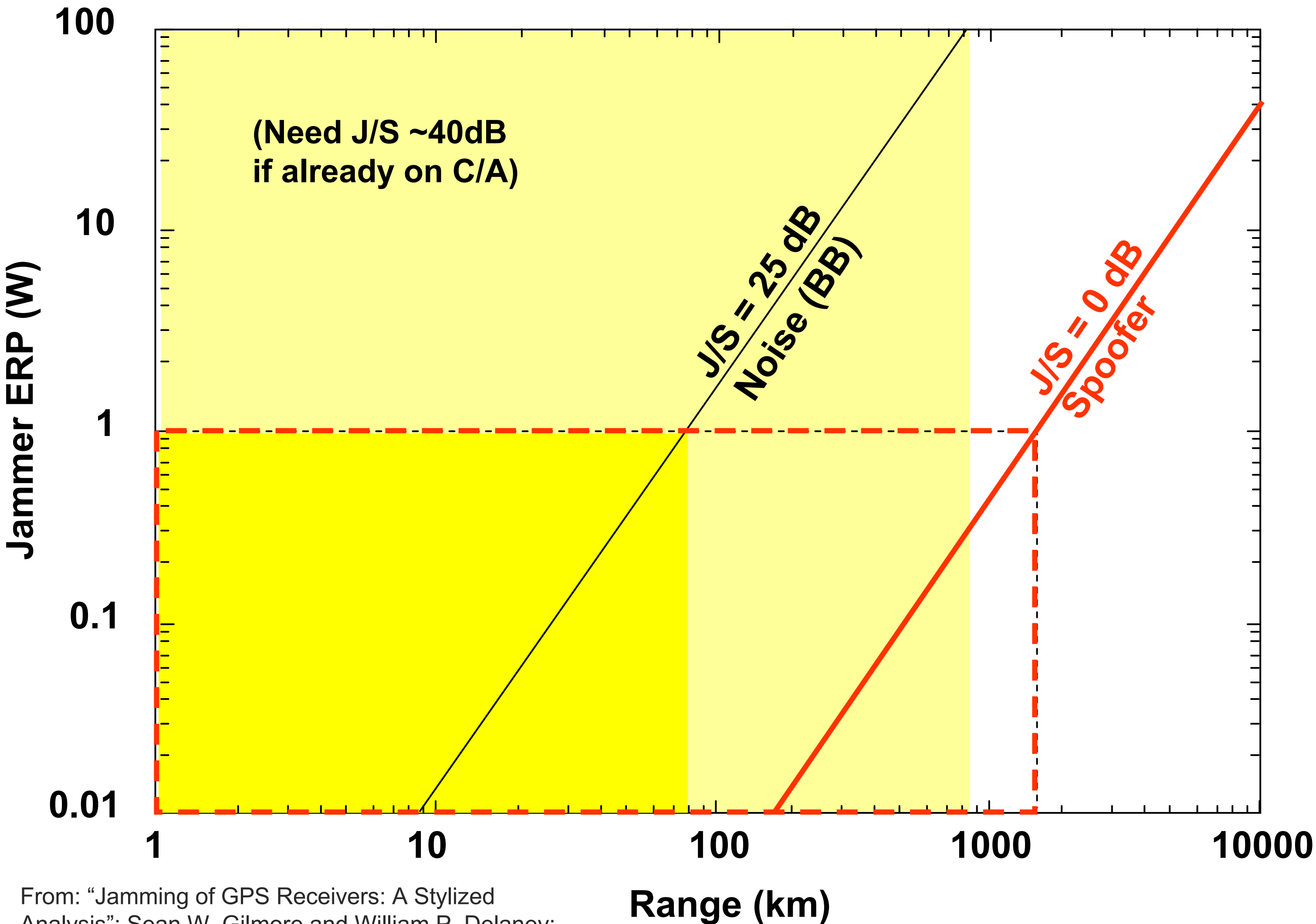




GPS Antenna:
12 Element
L-Band Helical
Phased Array
(On-axis view)



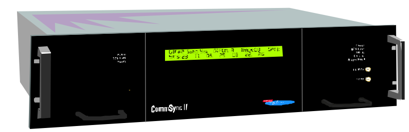
Jamming or Spoofing the GPS Civil (C/A) Signal



From: “Jamming of GPS Receivers: A Stylized Analysis”; Sean W. Gilmore and William P. Delaney; MIT Lincoln Lab; (Unclassified, non-FOUO Report)

Safeguarding against Loss of the GPS-C/A Signal

Cesiums (Primary Standards)



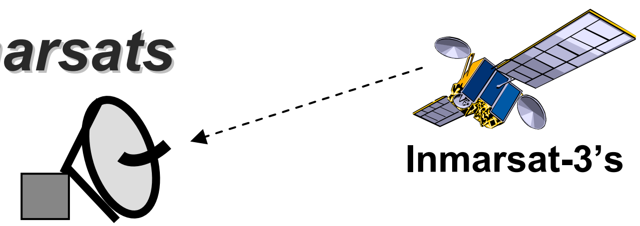
- ~$25K to $50K each
- Must be given time to keep

Loran-C Receivers

- Not Worldwide Coverage
- Next accuracy to GPS

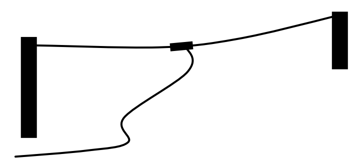
WAAS/EGNOS/MSAS/SNAS Inmarsats

- 10dB(+) Gain against J/S with 18” Dish
- Not a Total Solution for Jamming



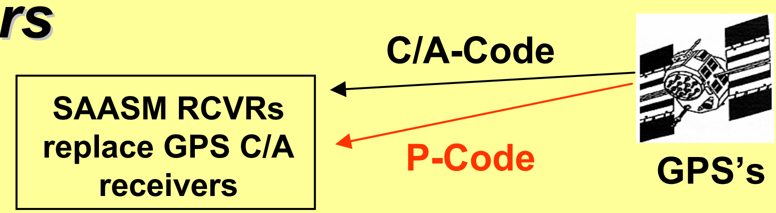
National (LF) Time Transmitters

- Not Worldwide Coverage
- Accuracies not close to Loran or GPS



SAASM-GPS P-Code Receivers

- Commercial applications possible
- Low Cost Alternative to Cs
- Requires COMSEC setup

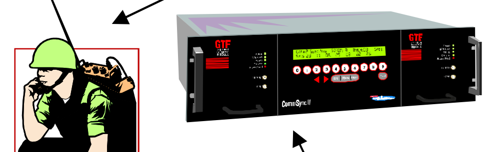
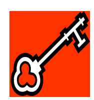
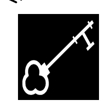
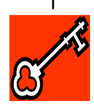
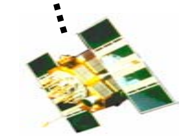


What is SAASM all about ?

Definitions

- **SAASM - Selective Availability Anti-Spoof Module**
  - **SA** – Selective Availability – a way to degrade the Civil C/A-Code Signal in case of strategic conflicts
  - **AS** – Anti-Spoof – a way to secure the precision Military P(Y)-Code Signal via cryptography to provide "Authorized Users Only" capability
  - **M** – Module
- **Direct P(Y) Acquisition**
  - Acquisition of the Military P(Y)-Code signal without dependence on the C/A-Code signal for accurate time

Pre-SAASM to SAASM Comparison

	Pre-SAASM HW and Keys were Classified	SAASM HW and SW Unclassified
P-CODE RECEIVER:	GPS PPS RECEIVER	Protected HW & SW → GPS PPS RECEIVER
HOST EQUIPMENT: (Portable or Stationary)		
KEYS: (Classified Red Key)		Encrypted Encryption KEY (Unclassified) 
RE-KEYING: (Manual)		RE-KEYING: (Automatic, Over-the- Air) 
SECURITY CONTROLS	COMSEC	Still must have COMSEC

The New Military GPS Infrastructure

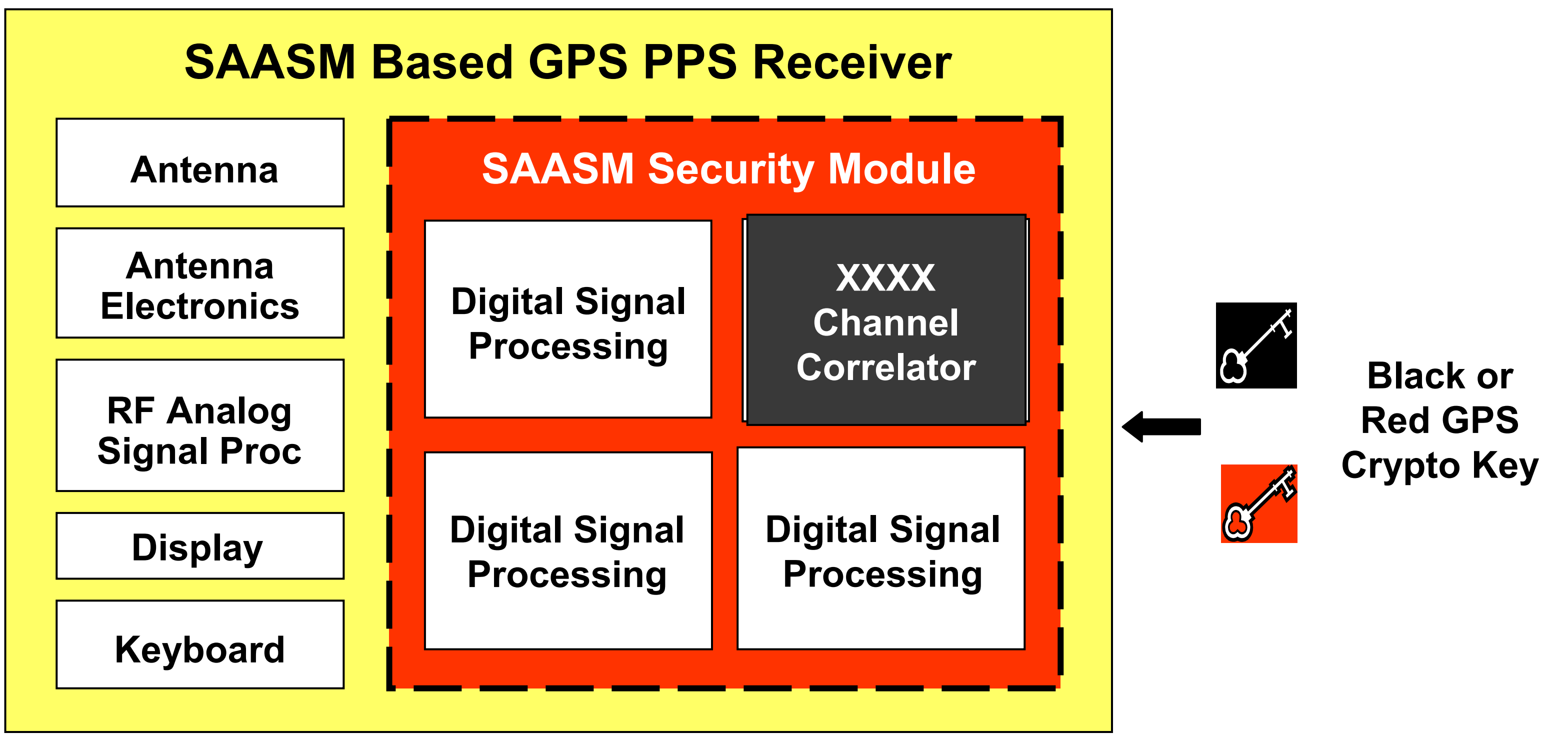
- Time has changed longstanding Cold War Strategic Threats to a new generation of Tactical Warfare and Terror- Induced conflicts
- The new generation military GPS infrastructure meeting this challenge is referred to as SAASM, which includes:
  - A **tamper-proof receiver** (both HW and SW), so that national security assets are protected in case of a receiver compromise
  - GPS equipment can now be **fielded as unclassified** to reduce logistic complexities
  - **Unclassified GPS keys** now available, again to reduce key management logistics
  - **Over-The-Air-Re-keying** via GPS messages, so that combatants remain keyed behind enemy lines
  - **Cyptonets,** allowing individual GPS keys to be assigned to authorized user groups
  - The ability to acquire the military P(Y) signal without the civil signal being available [**direct P(Y) acquisition** vs. pre-SAASM civil C/A first, then P(Y)]
  - A host of **classified systems capabilities** to greatly enhance the GPS SAASM functionalities

The New Military GPS Infrastructure

- Time has changed longstanding Cold War Strategic Threats to a new generation of Tactical Warfare and Terror- Induced conflicts
- The new generation military GPS infrastructure meeting this challenge is referred to as SAASM, which includes:
  - A **tamper-proof receiver** (both HW and SW), so that national security assets are protected in case of a receiver compromise
  - GPS equipment can now be **fielded as unclassified** to reduce logistic complexities
  - **Unclassified GPS keys** now available, again to reduce key management logistics
  - **Over-The-Air-Re-keying** via GPS messages, so that combatants remain keyed behind enemy lines
  - **Cyptonets,** allowing individual GPS keys to be assigned to authorized user groups
  - The ability to acquire the military P(Y) signal without the civil signal being available [**direct P(Y) acquisition** vs. pre-SAASM civil C/A first, then P(Y)]
  - A host of **classified systems capabilities** to greatly enhance the GPS SAASM functionalities

SAASM Hardware Security

- The creation of a virtually tamper-proof security boundary for sensitive electronics in the GPS receiver
- The primary reason the HW can be fielded unclassified



SAASM Software Security

- Crypto SW can only be loaded by the KLIF (KDP Loading and Installation Facility)

KLIF

CONTRACTOR PROVIDED FIXTURING

LOAD SAASM CRYPTO SOFTWARE

RECORD KEEPING for HAE

RECEIVER MANUFACTURER

TAMPER RESISTANT SAASM MCM

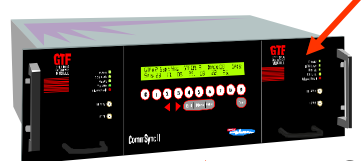
FINAL VENDOR SW LOAD

UNCLASSIFIED(1) WHEN KEYED

SAASM-BASED GPS PPS RECEIVER

OR RED KEY

UNCLASSIFIED BLACK KEY LOAD BY END-USER



SAASM HOST EQUIPMENT (HAE)

TO CUSTOMER

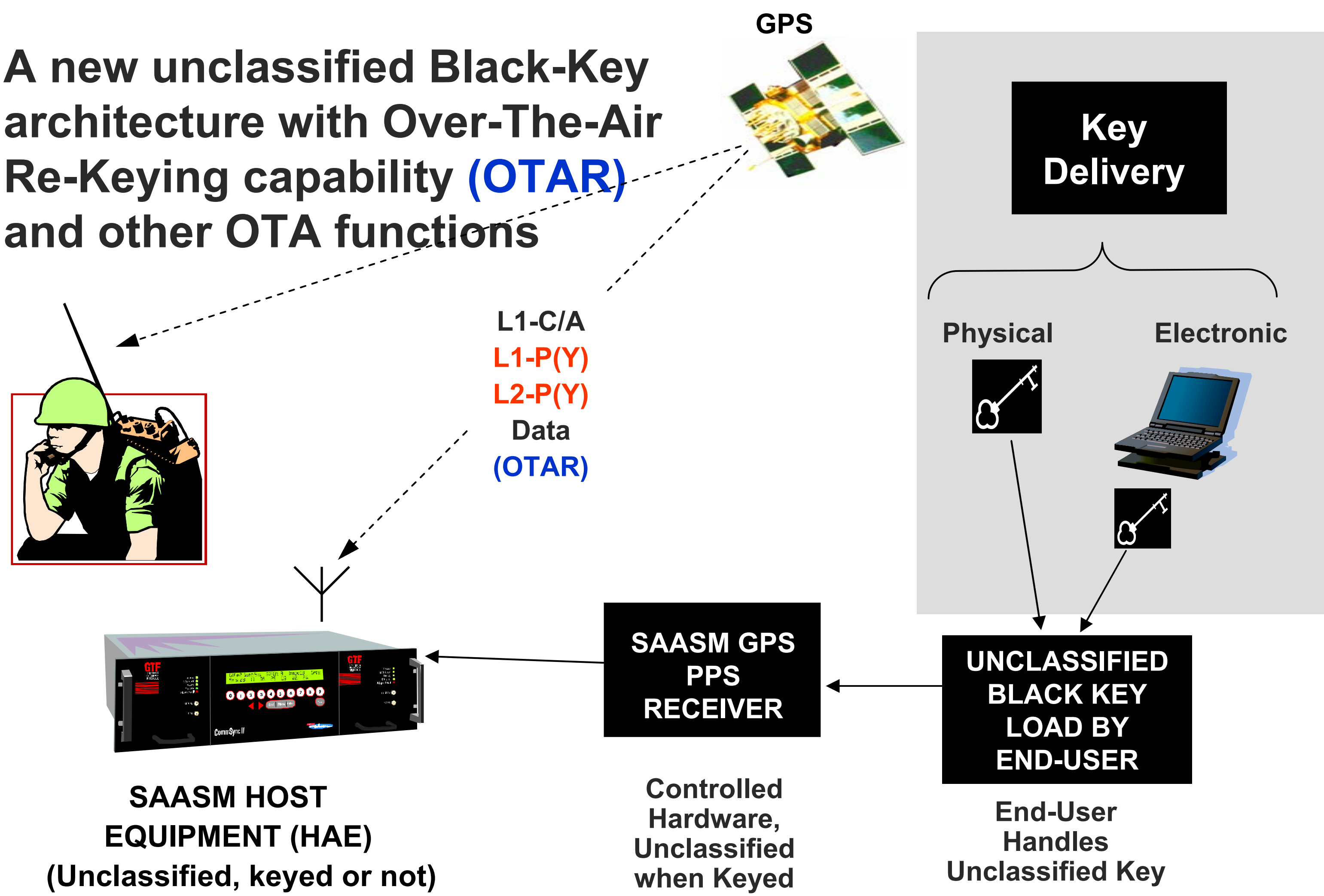
(1) Can only be defined Unclassified after GPS-JPO design review and approval; No Exceptions.

The New Military GPS Infrastructure

- Time has changed longstanding Cold War Strategic Threats to a new generation of Tactical Warfare and Terror- Induced conflicts
- The new generation military GPS infrastructure meeting this challenge is referred to as SAASM, which includes:
  - A **tamper-proof receiver** (both HW and SW), so that national security assets are protected in case of a receiver compromise
  - GPS equipment can now be **fielded as unclassified** to reduce logistic complexities
  - **Unclassified GPS keys** now available, again to reduce key management logistics
  - **Over-The-Air-Re-keying** via GPS messages, so that combatants remain keyed behind enemy lines
  - **Cyptonets,** allowing individual GPS keys to be assigned to authorized user groups
  - The ability to acquire the military P(Y) signal without the civil signal being available [**direct P(Y) acquisition** vs. pre-SAASM civil C/A first, then P(Y)]
  - A host of **classified systems capabilities** to greatly enhance the GPS SAASM functionalities

SAASM Black-Key Infrastructure

- A new unclassified Black-Key architecture with Over-The-Air Re-Keying capability (OTAR) and other OTA functions



The New Military GPS Infrastructure

- Time has changed longstanding Cold War Strategic Threats to a new generation of Tactical Warfare and Terror- Induced conflicts
- The new generation military GPS infrastructure meeting this challenge is referred to as SAASM, which includes:
  - A **tamper-proof receiver** (both HW and SW), so that national security assets are protected in case of a receiver compromise
  - GPS equipment can now be **fielded as unclassified** to reduce logistic complexities
  - **Unclassified GPS keys** now available, again to reduce key management logistics
  - **Over-The-Air-Re-keying** via GPS messages, so that combatants remain keyed behind enemy lines
  - **Cyptonets,** allowing individual GPS keys to be assigned to authorized user groups (FOUO)
  - The ability to acquire the military P(Y) signal without the civil signal being available [**direct P(Y) acquisition** vs. pre-SAASM civil C/A first, then P(Y)]
  - A host of **classified systems capabilities** to greatly enhance the GPS SAASM functionalities

The New Military GPS Infrastructure

- Time has changed longstanding Cold War Strategic Threats to a new generation of Tactical Warfare and Terror- Induced conflicts
- The new generation military GPS infrastructure meeting this challenge is referred to as SAASM, which includes:
  - A **tamper-proof receiver** (both HW and SW), so that national security assets are protected in case of a receiver compromise
  - GPS equipment can now be **fielded as unclassified** to reduce logistic complexities
  - **Unclassified GPS keys** now available, again to reduce key management logistics
  - **Over-The-Air-Re-keying** via GPS messages, so that combatants remain keyed behind enemy lines
  - **Cyptonets,** allowing individual GPS keys to be assigned to authorized user groups
  - The ability to acquire the military P(Y) signal without the civil signal being available [**direct P(Y) acquisition** vs. pre-SAASM civil C/A first, then P(Y)]
  - A host of **classified systems capabilities** to greatly enhance the GPS SAASM functionalities

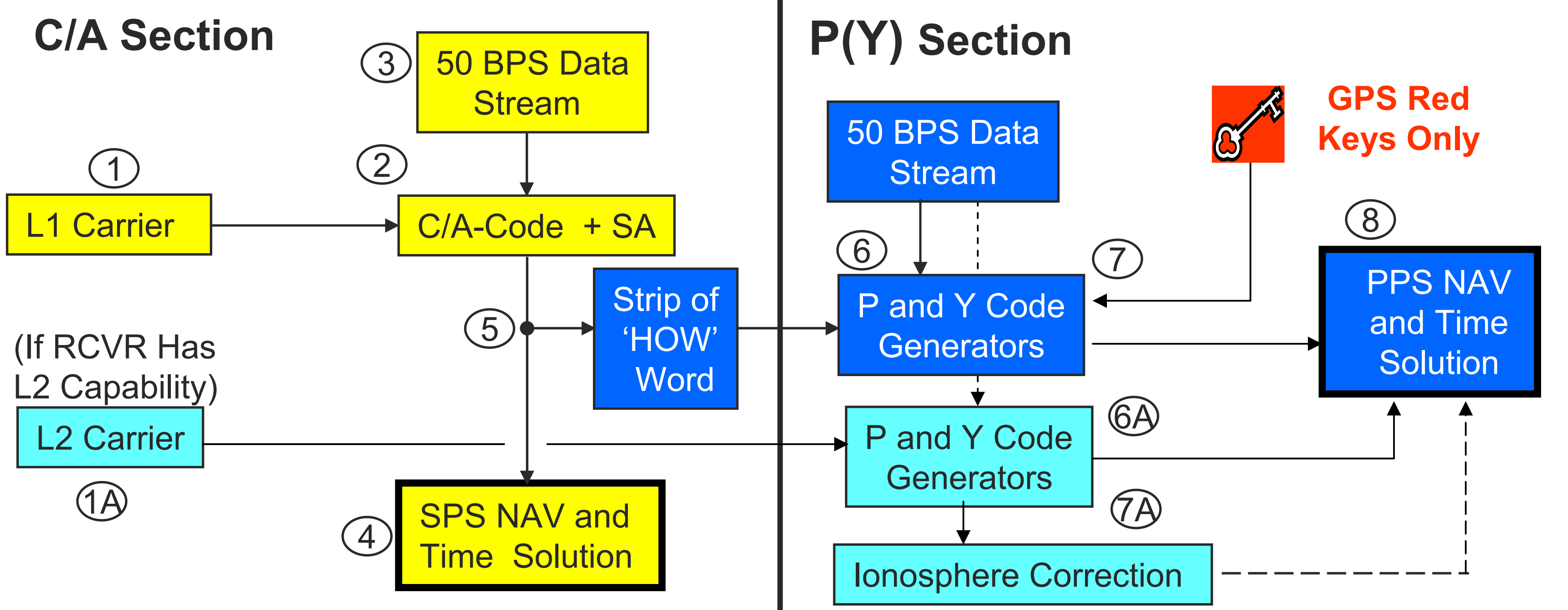
The New Warfare Realities

	Civil Signal C/A-GPS	Civil Signal C/A-GPS + Military Signal P(Y)-GPS
Users		
Cold War Strategic Conflict	**Use of SA to degrade C/A Civil Accuracy (Worldwide effect)**	**With C/A still available, no affect on military PPS Receivers**
Today's Tactical Conflicts	**C/A may not available, eliminating Civil use GPS (Local effect only)**	**Need to operate without C/A, Need Physical Security Need Direct-P(Y) Signal Acq.**

Pre-SAASM PPS RCVR P(Y) Signal Acquisition

SPS ~10m, 100 ns Time, 1σ
(Std. Positioning Service)
Civilian-User

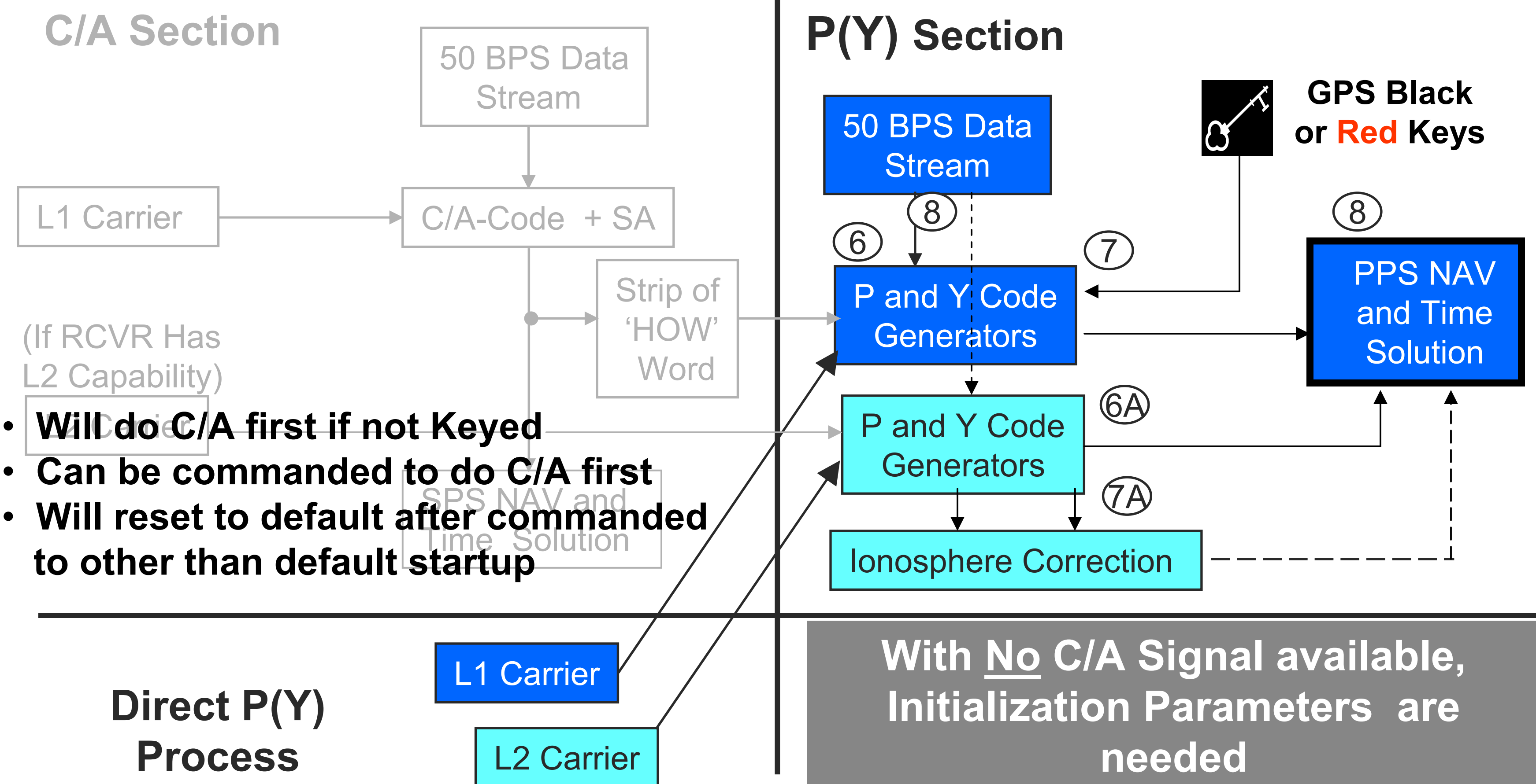
PPS ~3m, 50 ns Time, 1σ
(Precise Positioning Service)
Crypto-Authorized Users Only



With C/A Signal available, no Time or Initialization Parameters needed

SAASM PPS RCVR Direct P(Y) Signal Acquisition

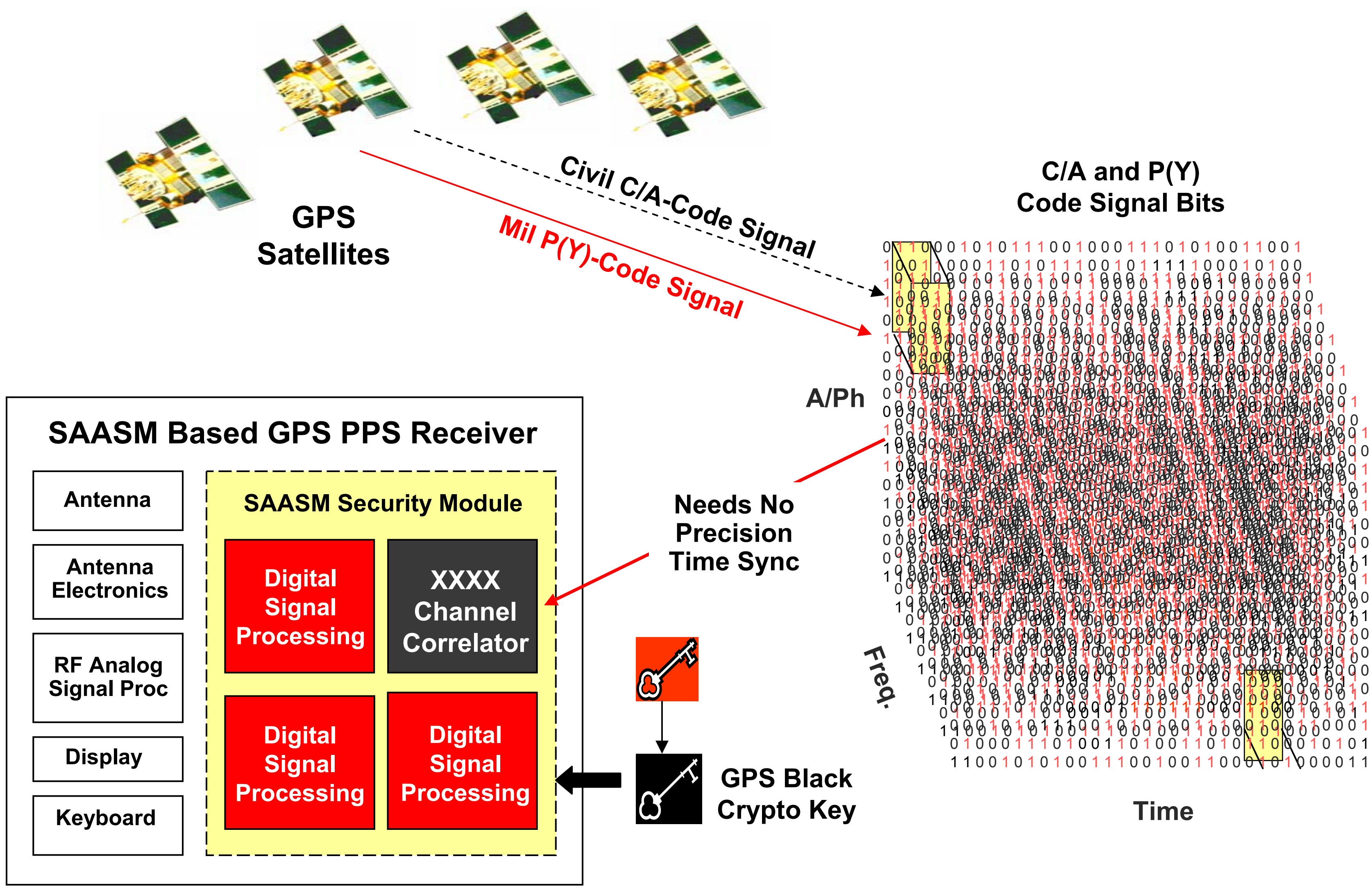
SPS ~10m, 100 ns Time, 1σ (Std. Positioning Service) Civilian-User	PPS ~3m, 50 ns Time, 1σ (Precise Positioning Service) Crypto-Authorized Users Only



- **Will do C/A first if not Keyed**
- **Can be commanded to do C/A first**
- **Will reset to default after commanded to other than default startup**

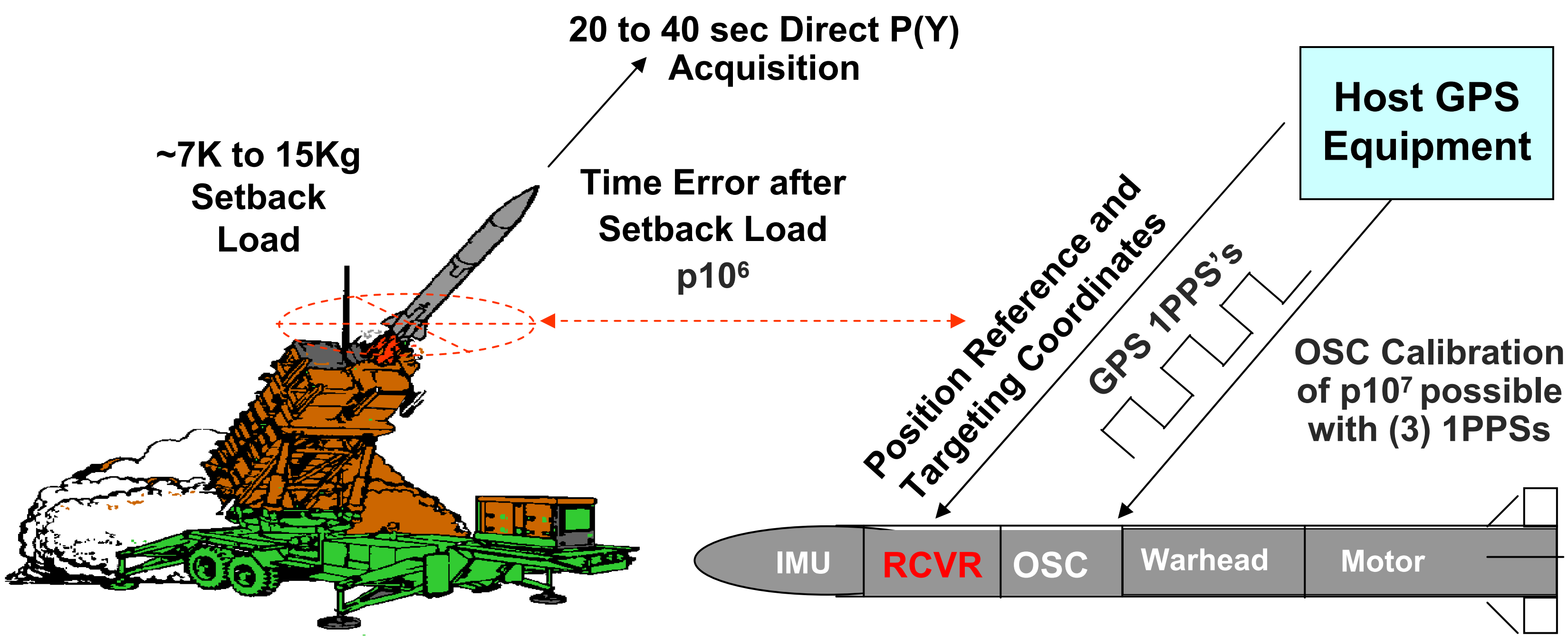
With No C/A Signal available, Initialization Parameters are needed

Direct P(Y) Signal Acquisition Correlator



Direct-P(Y) Receiver Applications
Weapons Platforms

1 to 10 ms Time Error for Initialization of the Direct P(Y) Receiver



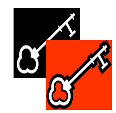
Typical Initialization Parameters for Direct P(Y) Acquisition	
Position Uncertainty	a few meters SEP
Velocity Uncertainty	N/A
Time Uncertainty	± 10s of microseconds
Almanac/Ephemeris	Most recent from Host

Direct-P(Y) Receiver Applications
Communications and Portable Users

Seconds of Time Error for Initialization of the Direct P(Y) Receiver

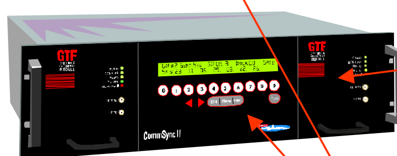
Hand-Held/Portable Units
PLGR, DAGR, other

GPS
Crypto
Key

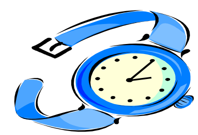


NO
Host GPS Equipment

Time/Frequency/Sync
Telecom Terminals



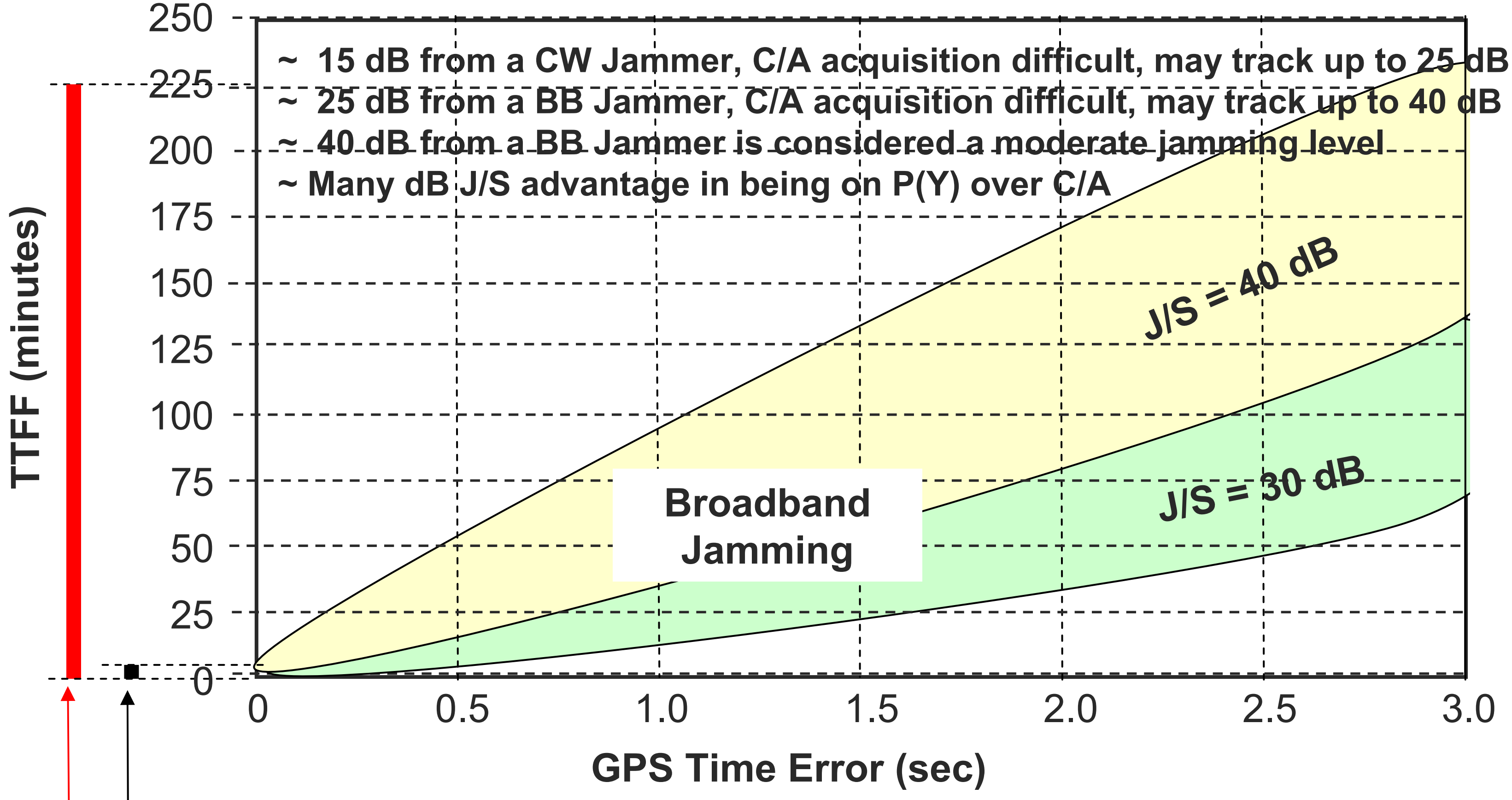
Manual input of
Parameters via
Keyboard



Typical Initialization Parameters for Direct P(Y) Acquisition

Position Uncertainty	< 100 Km Radius
Velocity Uncertainty	< 100 Km/h
Time Uncertainty	± 1 to 2 seconds
Almanac	Can be a Week Old

Approximation of TTFF vs. Time Error



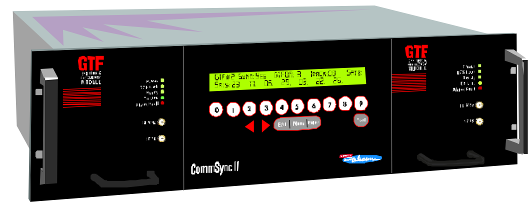
TTFF for Conventional SPS and PPS signal acquisition (with 100ns C/A Time)

TTFF for Direct-P(Y) acquisition, DEPENDING ON INITIALIZATION PARAMETERS

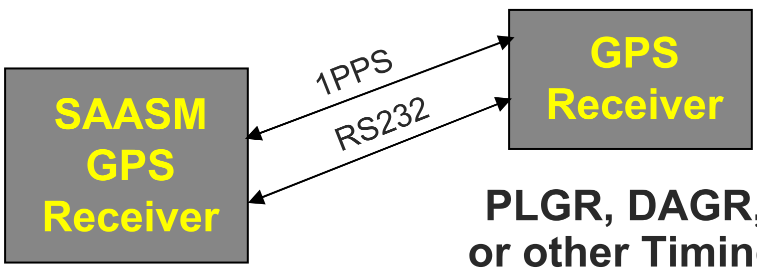
Time initialization methods for Direct-P(Y)

Using the Terminal's Hold-Over Oscillator

- Provides Time after 1st day to ~1us (Rb) and ~10us (Qz)
- Provides Latest Almanac
- Provides Latest Ephemeris
- Fastest TTFF
- No Connection required



Using another GPS PPS Receiver as the Host

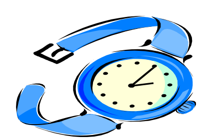


PLGR, DAGR, or other Timing Source

- Provides Time to <1ms
- Provides Latest Almanac
- Provides Latest Ephemeris
- Next Fastest TTFF
- Special Host RCVR Connection

Using Wristwatch

- Provides Time to ~ ±2 seconds
- Uses Last Almanac in Terminal RCVR
- Ephemeris derived from Almanac
- Slowest TTFF
- No Connection required

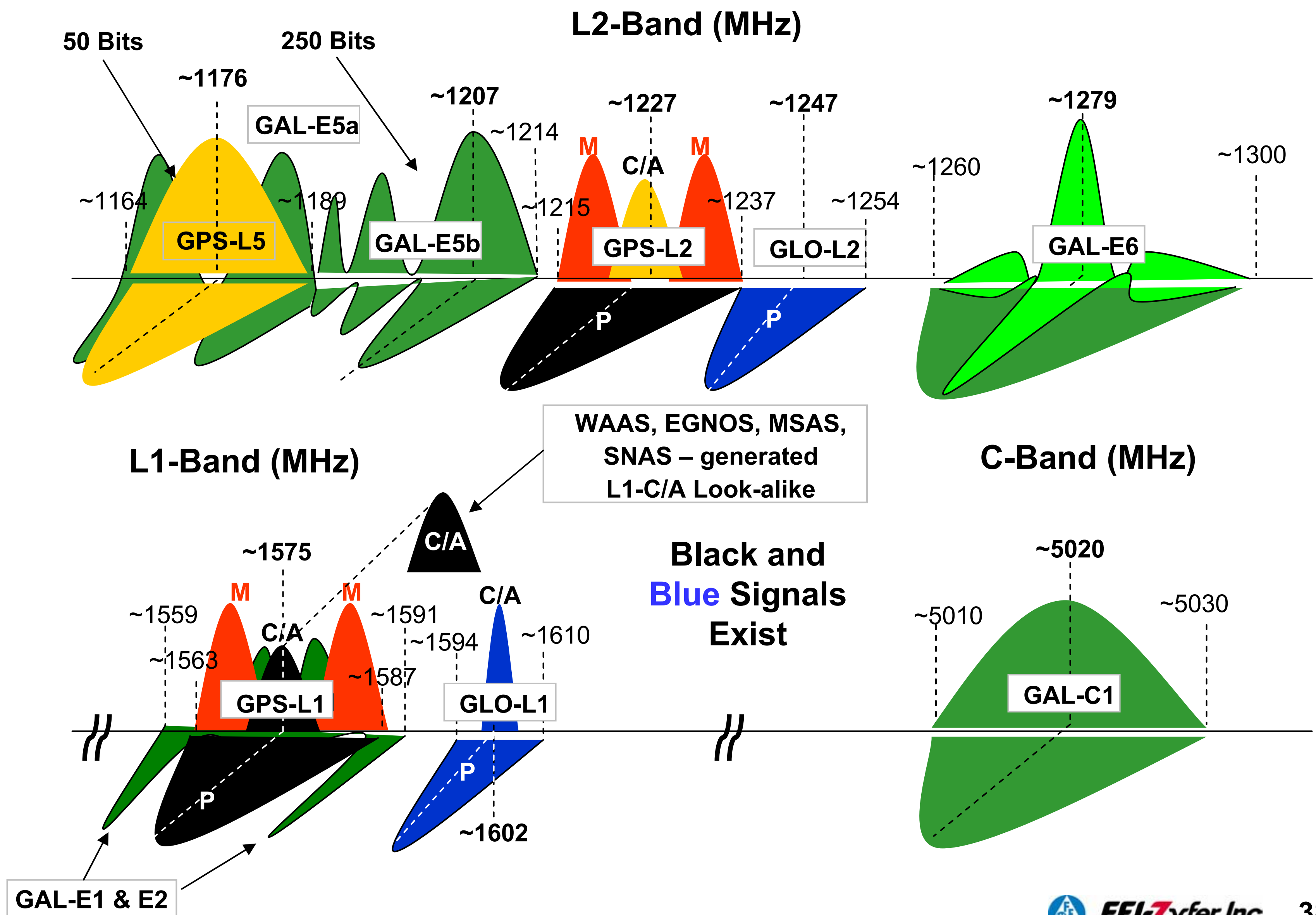


The New Military GPS Infrastructure

- Time has changed longstanding Cold War Strategic Threats to a new generation of Tactical Warfare and Terror- Induced conflicts
- The new generation military GPS infrastructure meeting this challenge is referred to as SAASM, which includes:
  - A **tamper-proof receiver** (both HW and SW), so that national security assets are protected in case of a receiver compromise
  - GPS equipment can now be **fielded as unclassified** to reduce logistic complexities
  - **Unclassified GPS keys** now available, again to reduce key management logistics
  - **Over-The-Air-Re-keying** via GPS messages, so that combatants remain keyed behind enemy lines
  - **Cyptonets,** allowing individual GPS keys to be assigned to authorized user groups
  - The ability to acquire the military P(Y) signal without the civil signal being available [**direct P(Y) acquisition** vs. pre-SAASM civil C/A first, then P(Y)]
  - A host of **classified systems capabilities** to greatly enhance the GPS SAASM functionalities

Future GPS and Galileo Signals

Available and Upcoming Signals for Telecom

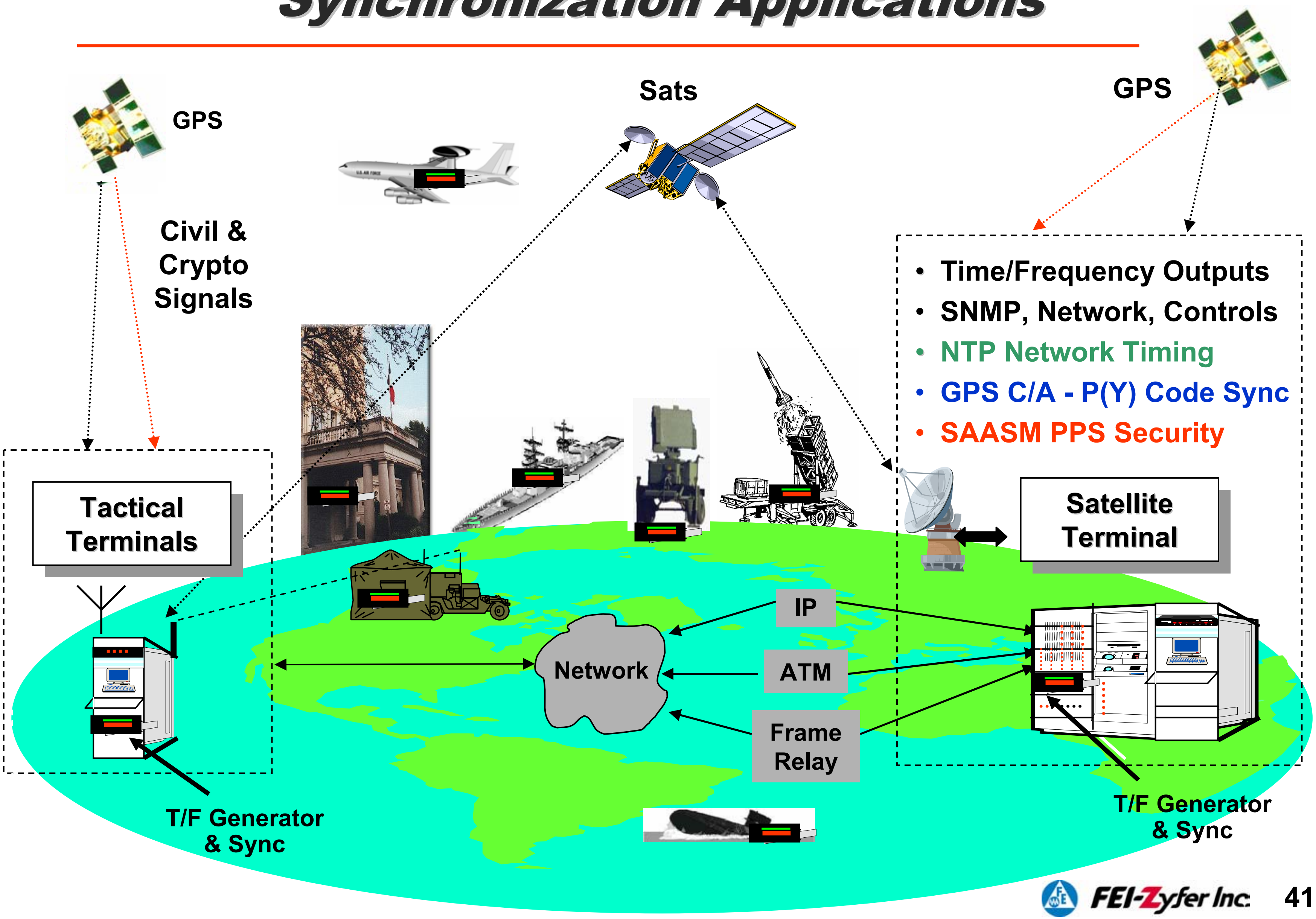


Future

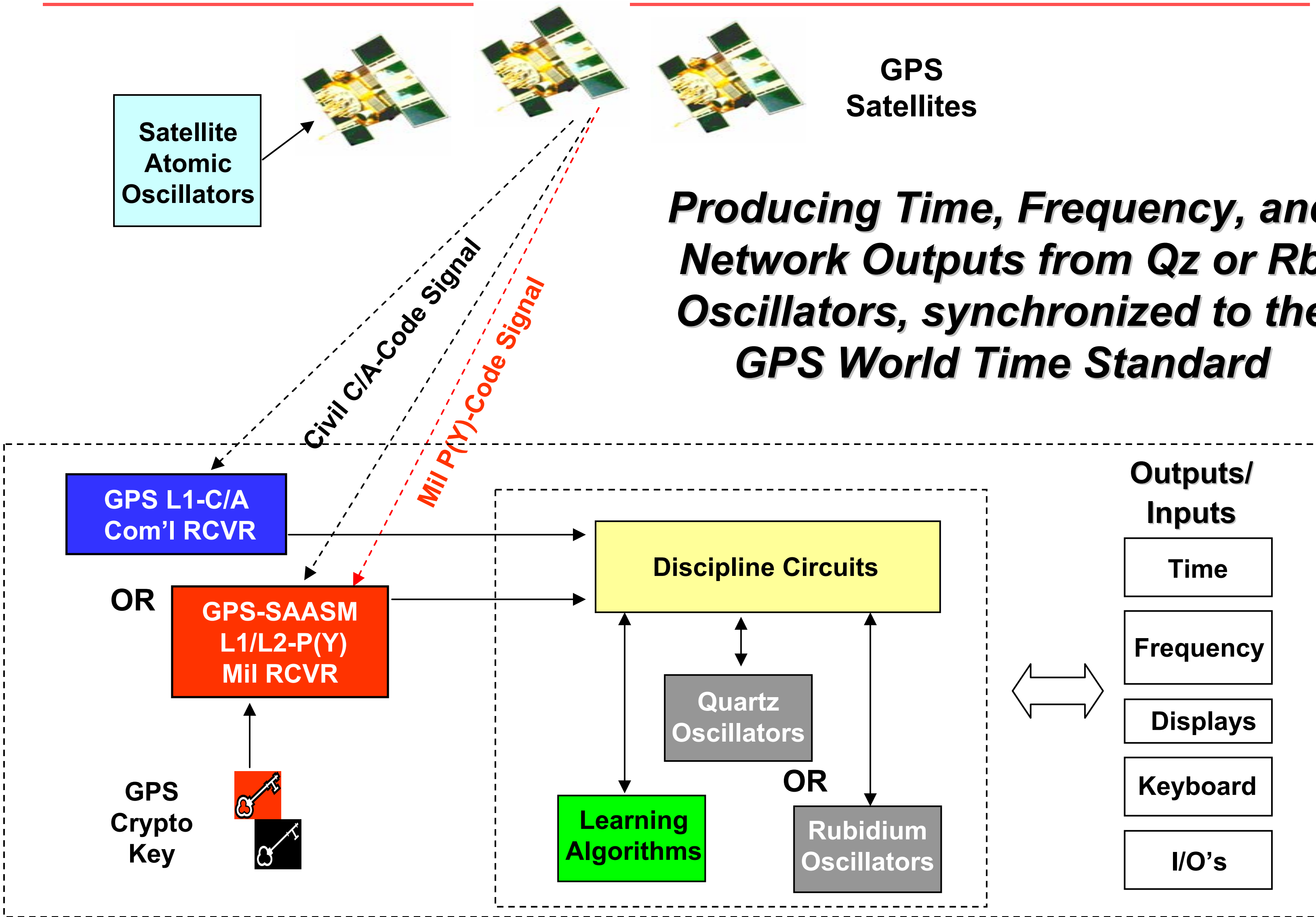
- New M-Code (or sometimes referred to as LM) architecture will most likely be an extension and upgrade to the SAASM receiver technology
- Further signal integration with the upcoming Galileo Constellation will most likely be part of backward compatible SAASM receivers

The GPS Sync Engine

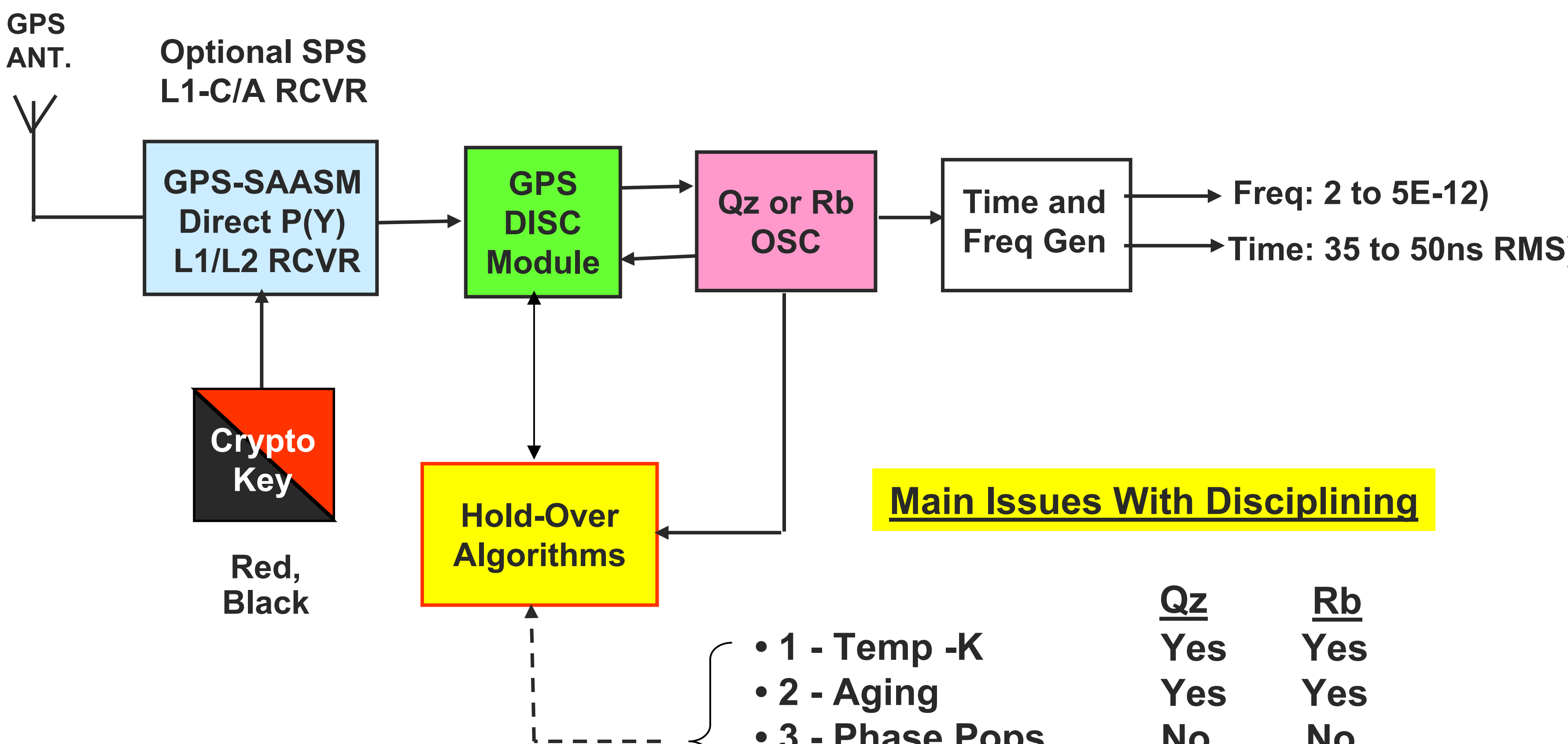
Communications and Command/Control Synchronization Applications



Building Blocks of FEI-Zyfer's Core Products



SAASM Time & Freq. Engine



Main Issues With Disciplining

	Qz	Rb
• 1 - Temp -K	Yes	Yes
• 2 - Aging	Yes	Yes
• 3 - Phase Pops	No	No
• 4 - P.S. Variations	No	No
• 5 - Holdover Model	Good	Better

GPS-SAASM Time/Frequency Generation and Synchronization Security

- ***Precision Frequency Generation***
  - Reference frequencies for Carriers, Radars, Signal Analysis, Test
- ***Precision Time Generation***
  - Spread Spectrum Transmissions (PN, FH, TH radios)
  - Data Analysis, Data Correlation, Time Stamping, Testing
- ***Time and Frequency Synchronization***
  - Spread Spectrum and Simulcast Communications
  - Coherent, High Data Rate (low BER) Communications
  - Network Communications/Data Synchronization
- ***Terminal Navigation and Positioning Solution***
- ***GPS-SAASM-aided Terminals vs. SPS or Std. PPS***
  - More difficult to Jam
  - Spoof-Proof
  - **Operate in the absence of civil C/A signal**
  - Comply with CJCS Mandate for the Government

Redundant SAASM CommSync II Modular Time & Frequency System (3U)

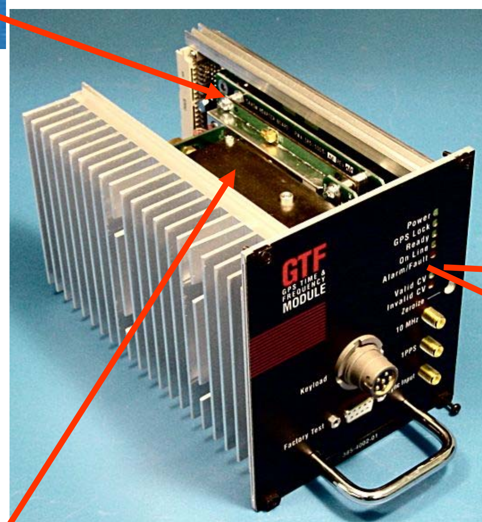
CommSync II
GTF Module

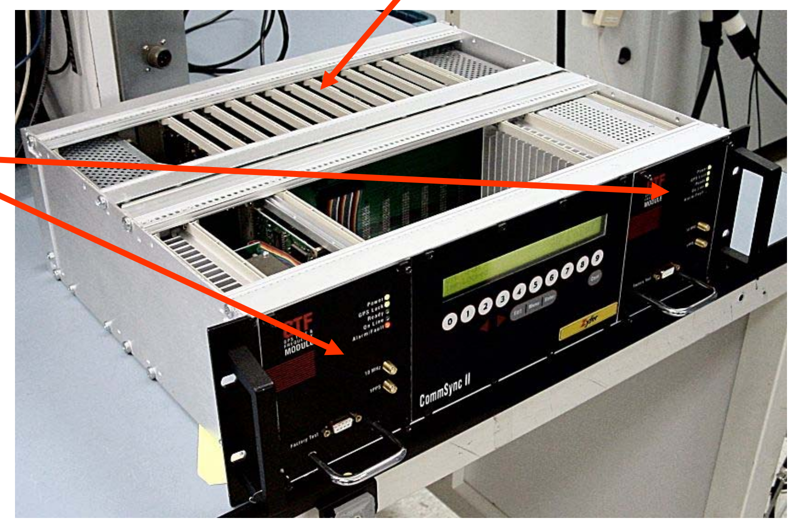
Plug-In
Output
Modules

Imbedded
SAASM
Receiver

OR

Commercial
C/A-Code
GPS RCVRs



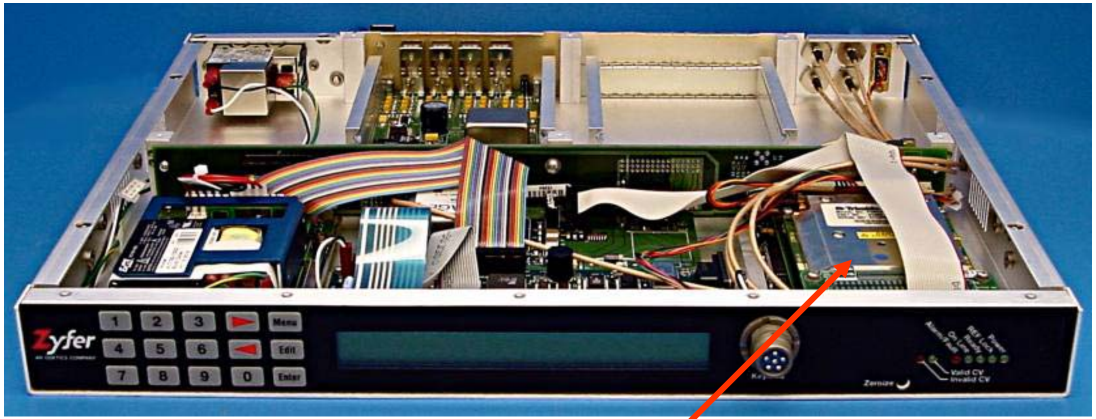


Atomic Oscillators

OR

Qz Oscillators

Single String SAASM GSync Modular Time & Frequency System (1U)



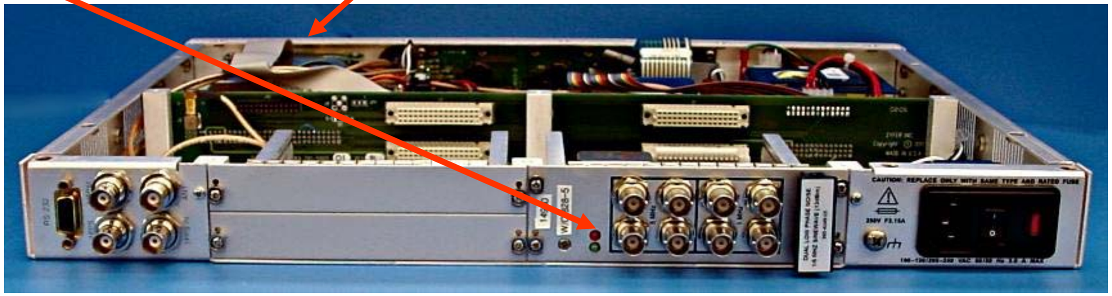
Plug-in Output Modules

Imbedded SAASM Receiver

OR

Commercial C/A-Code GPS RCVRs

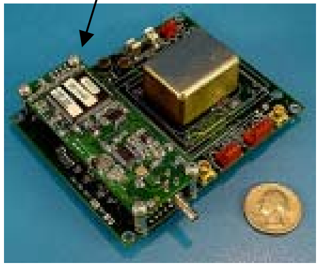
Ethernet & I/O Ports



GPS Time & Frequency Engines

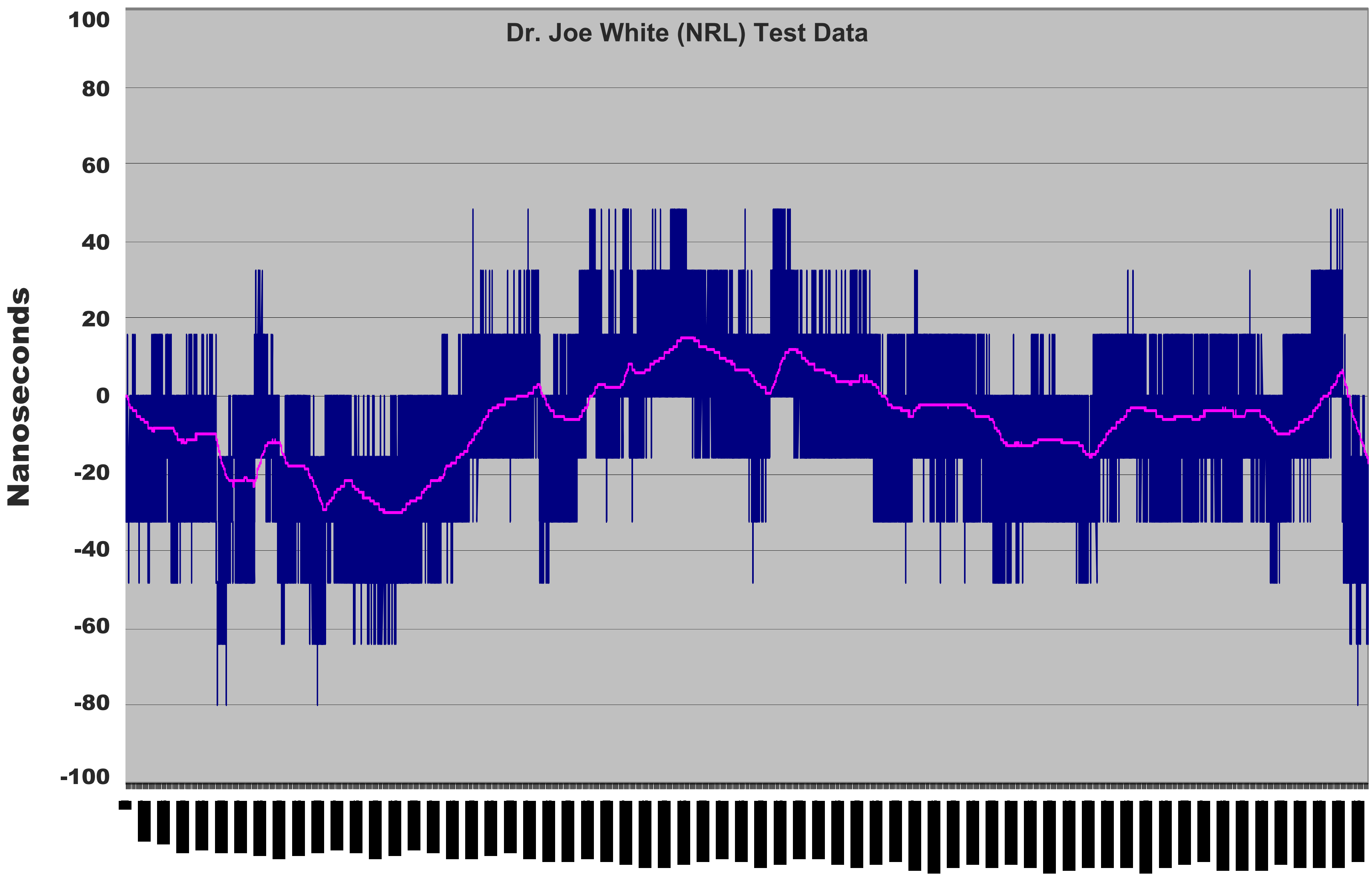
Can also come with
Imbedded SAASM Receiver

NanoSync



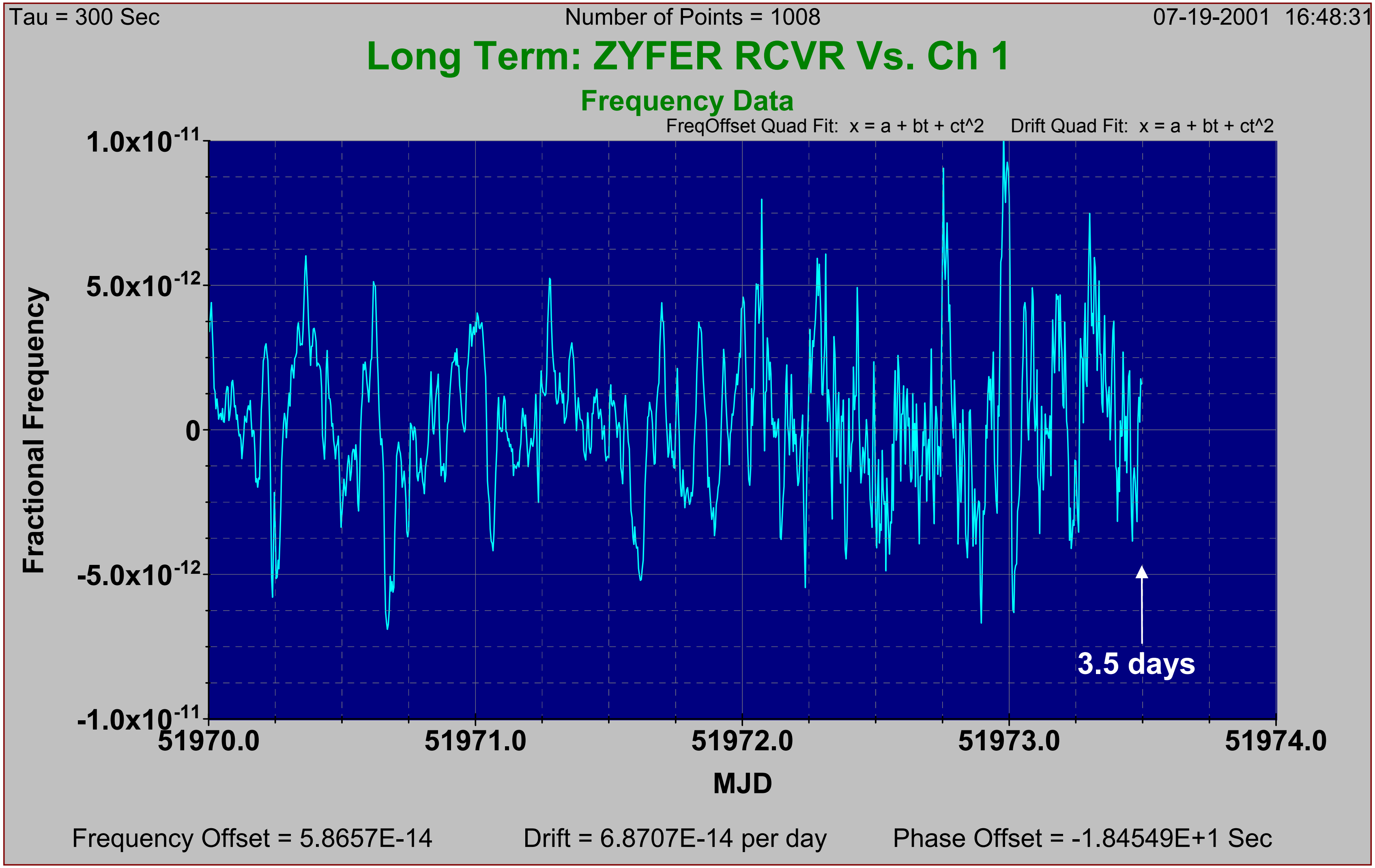
Sub-Systems and Modules for Special Purpose Applications

Typical Time Error – with GPS-P(Y)



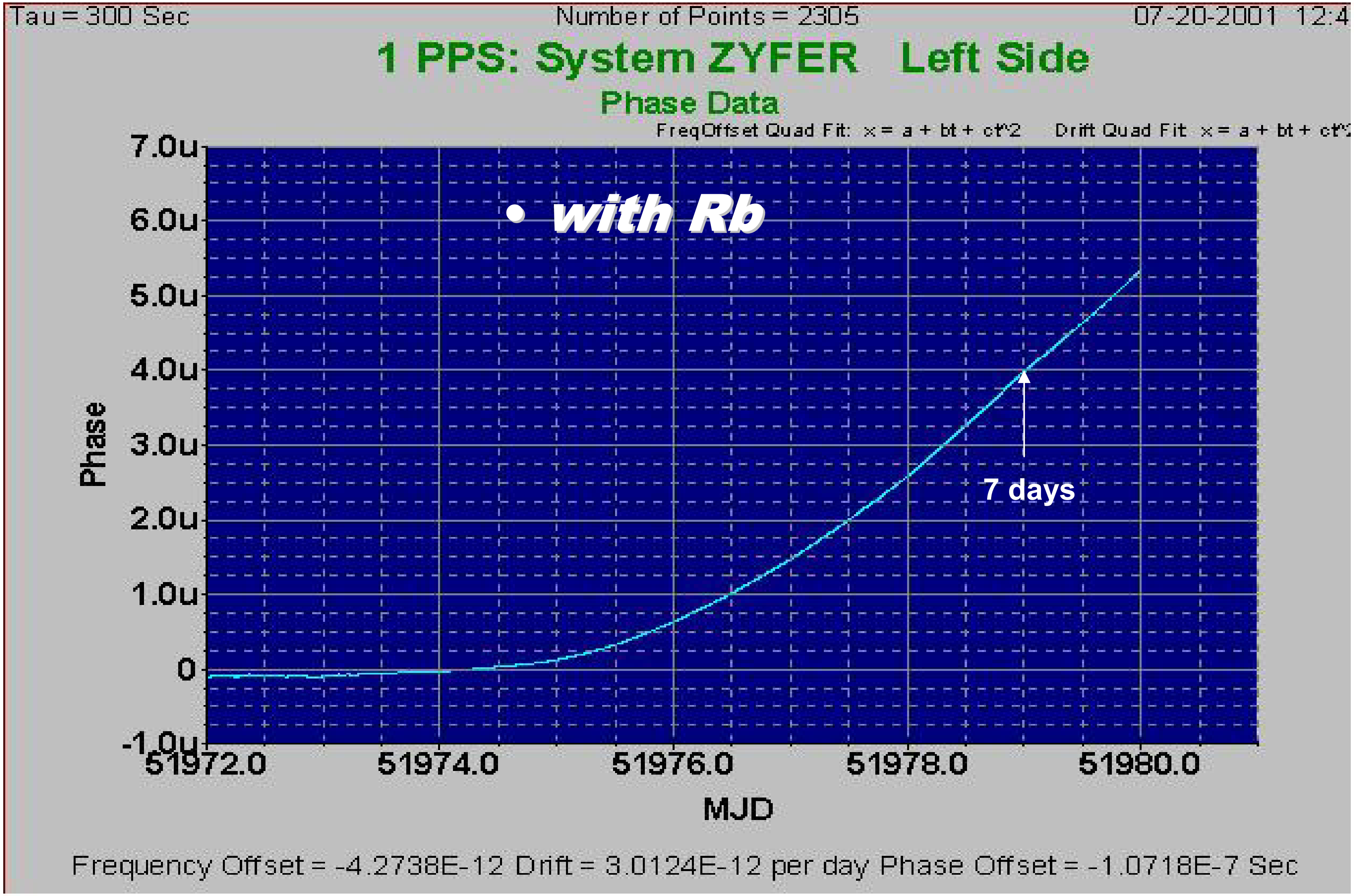
Typical Frequency Offset – with GPS-P(Y)

Dr. Joe White (NRL) Test Data



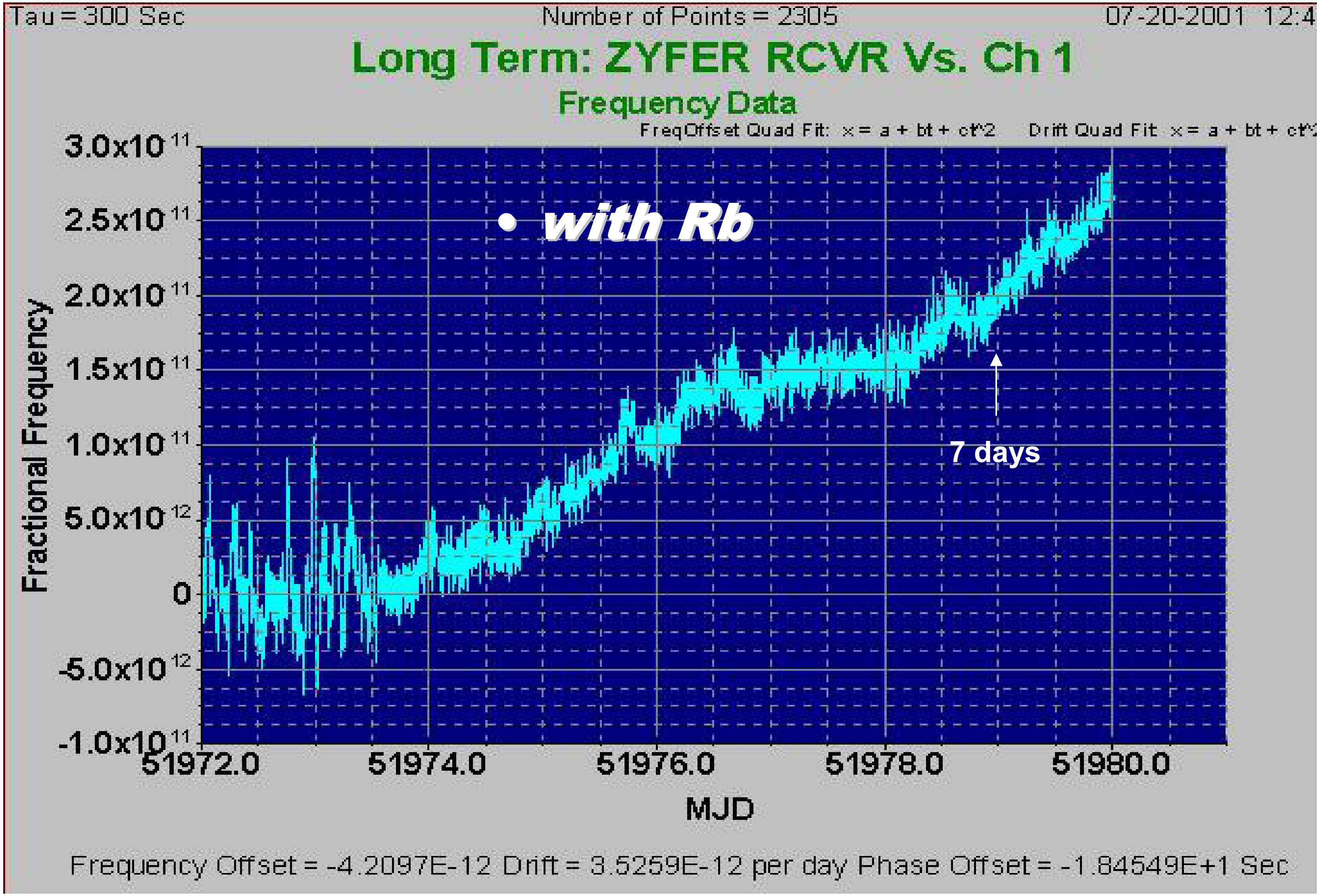
Typical Holdover Time Error (no GPS)

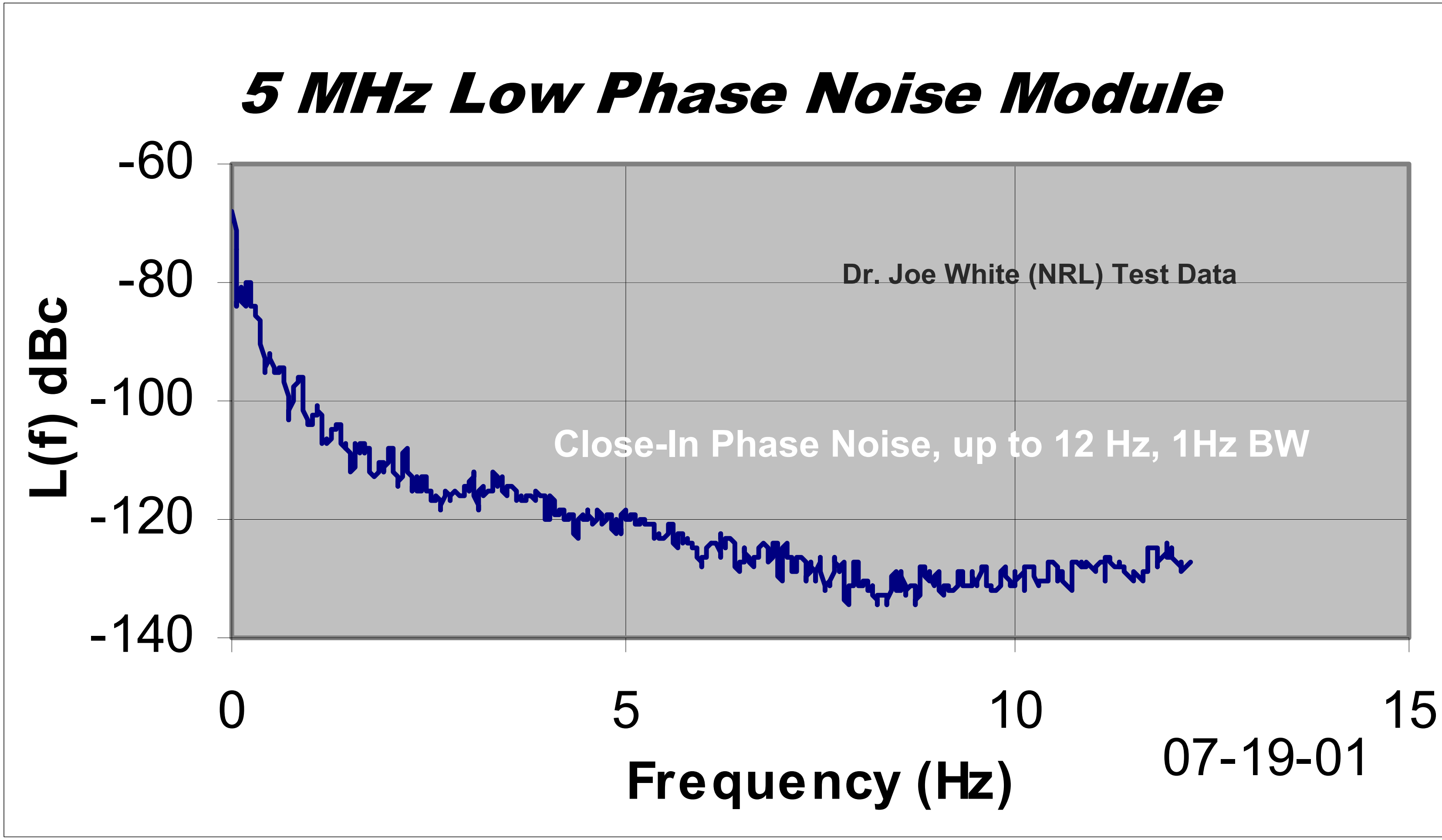
Dr. Joe White (NRL) Test Data



Typical Holdover Frequency Error (no GPS)

Dr. Joe White (NRL) Test Data





Frequency Offset	1 Hz	10 Hz	100 Hz	1 kHz	10 kHz	100kHz
Low Noise Specification	-102	-127	-140	-147	-152	-152
Standard Module	-88	-101	-119	-122	-138	-141
Low Noise Module	**-103**	**-130**	**-140**	**-151**	**-156**	**-158**
Reference Oscillator	-120	-150-	-170	-170		

DEPARTMENT OF THE AIR FORCE
HEADQUARTERS SPACE AND MISSILE SYSTEMS CENTER (AFMC)
LOS ANGELES, CA

MEMORANDUM FOR Zyfer Inc., an Odetics Company
1585 S. MANCHESTER AVE
ANAHEIM CA, 92802-2907
ATTN: STEVEN STRANG

FROM: SMC/CZU
2435 Vela Way, Suite 1613
Los Angeles AFB
El Segundo CA 90245-5500

SUBJECT: Security Approval of GPS PPS Host Application Equipment

1. As a result of successful completion of the NAVSTAR Global Positioning System (GPS) Selective Availability Anti-Spoofing Module (SAASM) based Host Application Equipment (HAE) Security Approval Process, the GPS Joint Program Office (JPO) hereby grants security approval for the following GPS PPS HAE hardware (H/W) and software (S/W):

Model Name	Part Numbers	Security Classification
CommSync-II, GTF Module	H/W: System: 385-4002-XX S/W: Security Core: 385-3028	Unclassified (Controlled) when keyed

2. This approval applies to only the part numbers identified above. The above hardware system part number includes X-digits representing potential variations to the approved hardware that do not affect the security characteristics of the HAE. Such variations are also approved. Any variation or derivative of the above hardware and software that do affect the security characteristics of the HAE shall be separately approved by the GPS Joint Program Office.

3. The above version of the CommSync-II, GTF Module shall contain one (1) Trimble Force 22 [H/W PN: 41205-XX, S/W PN: 1.XU]. Any derivatives of the contained Force 22 shall require separate security approval.

4. The above version of the CommSync-II, GTF Module is approved for red-key use only using KDP OPSW 0.9. OPSW 1.0 shall require separate approval.

5. Advertisements for these HAE may include the statement: "The (insert HAE name and/or model number) has been granted the NAVSTAR Global Positioning System Joint Program Office Security Approval."

6. Please note that these HAE may not be sold, loaned, leased, or otherwise provided to any other organization without prior GPS Joint Program Office authorization.

7. Should you have any questions regarding this approval, please contact Lt Jason Golaboski at (310) 363-0947.

received
5/4/01

Arnel B. Enriquez
for CATHERINE M. McGINN, Lt Col, USAF
Acting Program Manager, GPS User Equipment
NAVSTAR GPS Joint Program Office

Navstar GPS Joint Program Office (GPS-JPO)

Letter for FEI-Zyfer Inc. as an approved SAASM HAE Supplier for the:

CommSync-II, GTF Module HAE

DEPARTMENT OF THE AIR FORCE
HEADQUARTERS SPACE AND MISSILE SYSTEMS CENTER (AFSPC)
LOS ANGELES AIR FORCE BASE CALIFORNIA

05 AUG 2002

MEMORANDUM FOR ZYFER INC., AN ODETICS COMPANY
1585 SOUTH MANCHESTER AVE
ANAHEIM, CA 92802-2907
ATTN: STEVE STRANG

FROM: SMC/CZU
2420 Vela Way, Suite 1467
Los Angeles AFB
El Segundo CA 90245-4654

SUBJECT: Security Approval of SAASM Host Application Equipment

1. The GPS Joint Program Office (JPO) hereby grants security approval for the following GPS PPS HAE hardware (H/W) and software (S/W).

HAE Name	Hardware System Part Number	Software Part Number	Classification When Keyed
GSYNC	391-2XX-XX	385-3028	Unclassified (Controlled)

2. This security approval is based solely upon the information and material presented by the equipment developer to the GPS Joint Program Office in accordance with CZE-93-105A, Navstar GPS PPS HAE Security Approval Requirements and CZE-93-105A-SAASM, Tailoring of Security Approval Requirements for SAASM HAE. This security approval only applies to the developer's compliance with the GPS security requirements specified in the referenced document. It does not apply to any other hardware or software requirements. The GPS Joint Program Office does not certify or guarantee the functionality, performance, or quality of the equipment.

3. The above GSYNC, H/W Part #391-2XX-XX, is approved for use with Trimble Force-22, H/W Part # 41205-XX, and S/W Part #1.XU and the Trimble Navigation SAASM, Part # 38752-10-1X1X. The GSYNC is approved for red key use only with Key Data Processor (KDP) Developmental Test Software (DTSW). Use of Operational Software (OPSW Version 1.0) shall require separate approval.

4. Should you have any questions regarding this approval, please contact Lt Scott Schweitzer at (310) 363-3881.

RAKESH N. DEWAN, Colonel, USAF
Program Manager, GPS User Equipment
Navstar GPS Joint Program Office

GUARDIANS OF THE HIGH FRONTIER

Navstar GPS Joint Program Office (GPS-JPO)

Letter for FEI-Zyfer Inc. as an approved SAASM HAE Supplier for the:

GSYNC HAE

Important SAASM Documents

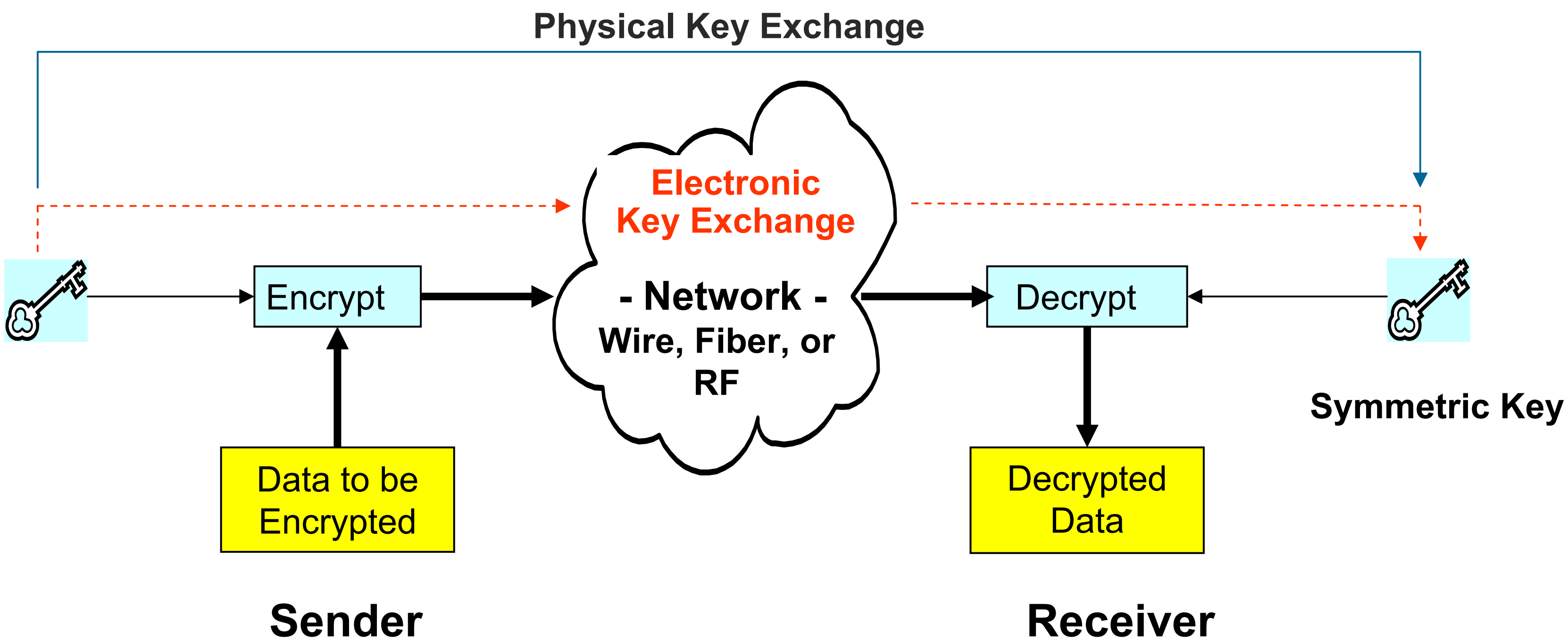
Additional Information on SAASM

- Most SAASM-related documents are FOUO
- Visit the SAASM website at www.gpsjpo.com/uesecurity
- The GPS-JPO provides an access password for this website for all qualified applicants

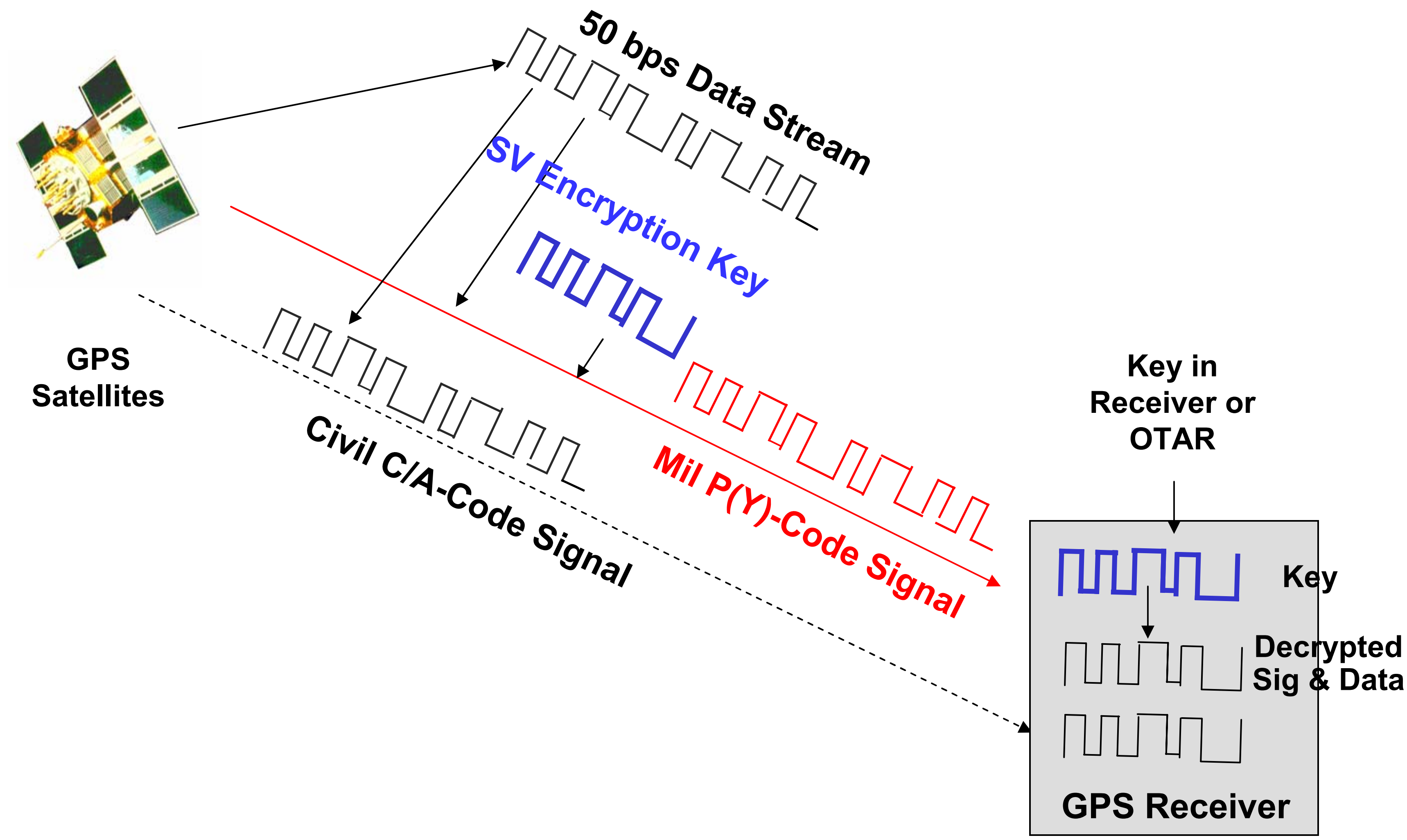
GPS Keying Basics

Symmetric Cryptography Basics

Symmetric Key must be exchanged first, physically or electronically



Basic Cryptography for GPS



GPS Keys

Crypto Key details are FOUO

Key Ordering Details

GPS Security Controlling Authority

HQ United States Space Command (USSPACECOM)

GPS COMSEC Manager
250 S. Peterson Blvd STE 116
Peterson AFB, CO 80914-3050

Primary POC: Mr. Martin Ferrante
DSN: 692-5022 / COM: 719-554-5022

Alt POC: MSgt Mary Grier
DSN: 692-9613 / COM:719-554-9613

Alt. POC: TSgt Tony Cravens
DSN: 692-6872 COM: 719-692-6872

FAX: Unclass – DSN 692-6314 Secure – DSN 692-7634
PLA: GPS COMSEC Manager Peterson AFB CO//

Security Validating Authorities

US Department of Defense

US Air Force (USAF)

HQ AFSPACECOM/DOGS
150 Vandenberg St, STE 1105
Peterson AFB, CO 80914-4200
PLA: HQ AFSPACECOM Peterson AFB CO//DOGS//

US Army (USA)

DIR USACCSLA
Attn: SELCL-KP-Key
Ft. Huachuca, AZ 85613-7090
PLA: DIRUSACCSLA FT HUACHUCA AZ//SELCL-KP-KEY//

Security Validating Authorities (Cont)

US Navy (USN)

Commander Naval Space Command
Attn: N312
Bldg. 1700
Dahlgren, VA 22448-5170
PLA: COMNAVSPACECOM DAHLGREN VA//N312//

US Marine Corps (USMC)

HQ US Marine Corps/CSBT7
2 Navy Annex
Washington DC, 20380-1775
PLA: CMC WASHINGTON DC//CSBT//

US Coast Guard (USCG)

USCG Telecommunications and Information Command
Command/OPS4
7323 Telegraph Road
Alexandria, VA 22310-3999
PLA: COGUARD-TISCOM ALEXANDRIA VA//OPS4//

Getting Setup for GPS-P(Y) Code Operation

COMSEC Room Setup & Clearance

Secure Room and Security Services for the Room

COMSEC Custodian Clearances

Security Training Sessions, etc.

Obtain COMSEC Account

NSA Filings, etc.

Order BCVm or BGUV2 GPS Keys

For GPS P(Y)-Code Operations, Monthly/Yearly Keys

Key Loading Devices

KOI-18, KYK-13, CYZ-10, 1553 Bus, Ethernet, etc.

Physical Devices or Network Keying (yet to be defined)

Physically or Electronically key the GPS RCVR

Key retention method specified in the RCVR KDP load IP

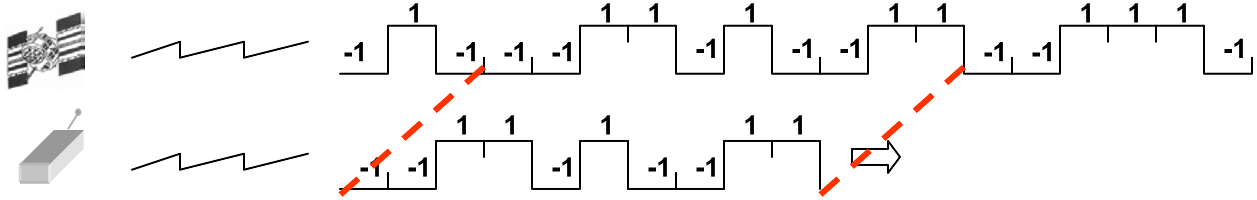
Once physically validated & authenticated, then OTAR capable

GPS Signal Acquisition

The Autocorrelation Function

Satellite C/A-Code

User Set matching C/A-Code



Autocorrelation Function $\frac{1}{N}\sum_{S=U}^{N} X_S \bullet X_U$

In the case above:

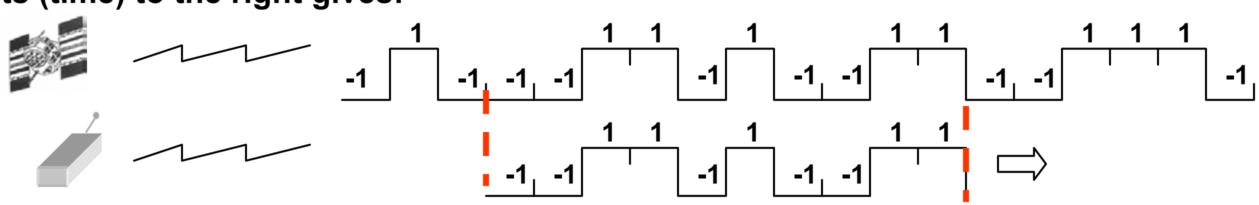
$$\frac{1}{10}\sum_{S=U}^{10} X_S \bullet X_U = (-1)(-1)+(1)(-1)+(-1)(1)+(-1)(1)+(-1)(-1)+(1)(1)+(1)(-1)+(-1)(-1)+(1)(1)+(-1)(1)$$

$$= \frac{1}{10}(+1-1-1-1+1+1-1+1+1-1) = 0$$

Shifting 3 bits (time) to the right gives:

Satellite

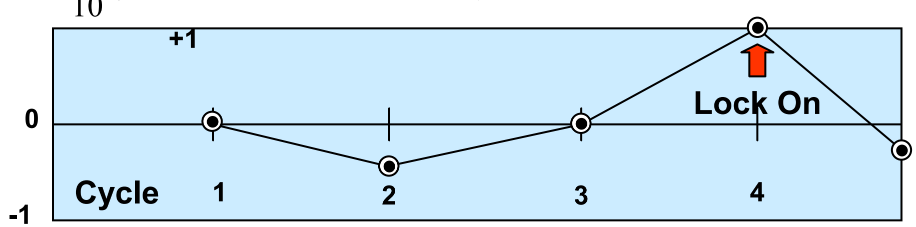
User Set



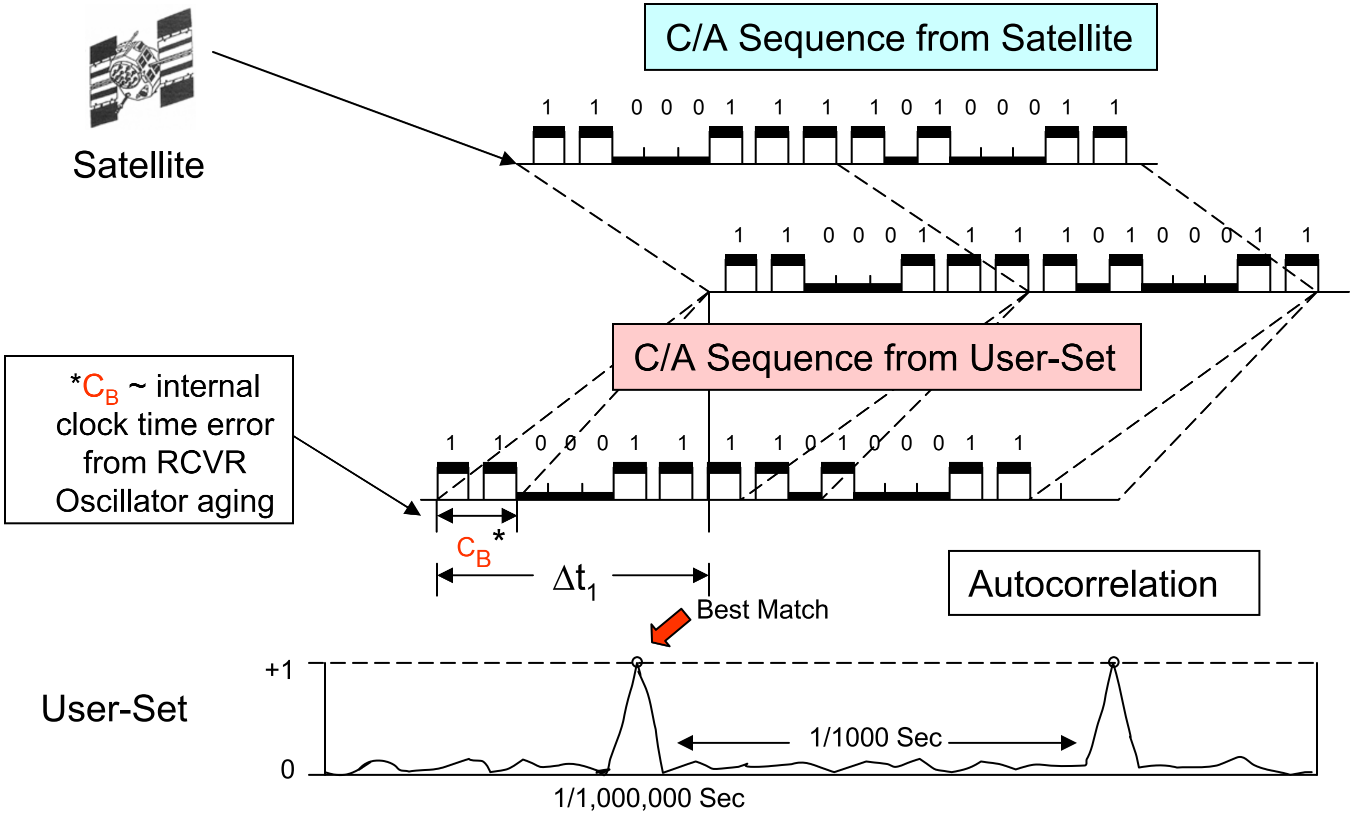
$$\frac{1}{10}\sum_{S=U}^{10} X_S \bullet X_U = (-1)(-1)+(-1)(-1)+(1)(1)+(1)(1)+(-1)(-1)+(1)(1)+(-1)(-1)+(-1)(-1)+(1)(1)+(1)(1)$$

$$= \frac{1}{10}(1+1+1+1+1+1+1+1+1+1) = 1$$

Autocorrelation Value



Acquiring the Clear Civil C/A Signal



Pseudo Ranges:

$R_1 = C\Delta t_1$

$R_2 = C\Delta t_2$

$R_3 = C\Delta t_3$

$R_4 = C\Delta t_4$

Position Equations:

$(X_1 - U_X)^2 + (Y_1 - U_Y)^2 + (Z_1 - U_Z)^2 = (R_1 - C_B)^2$

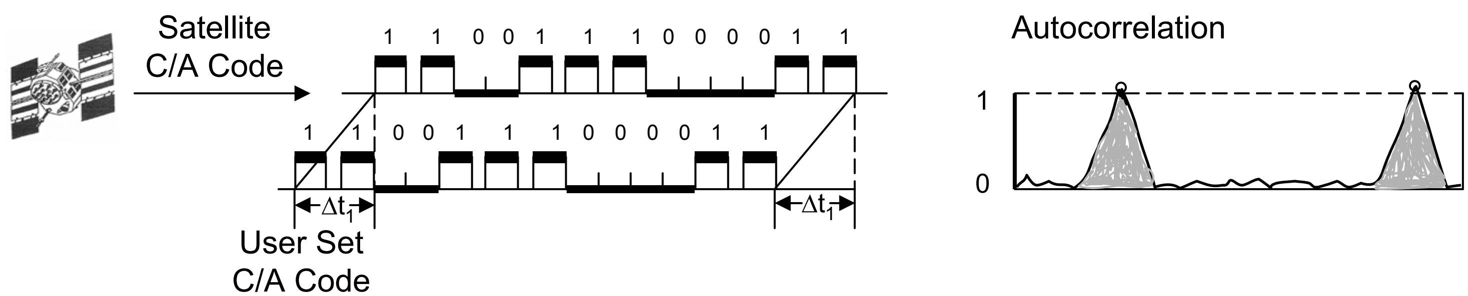
$(X_2 - U_X)^2 + (Y_2 - U_Y)^2 + (Z_2 - U_Z)^2 = (R_2 - C_B)^2$

$(X_3 - U_X)^2 + (Y_3 - U_Y)^2 + (Z_3 - U_Z)^2 = (R_3 - C_B)^2$

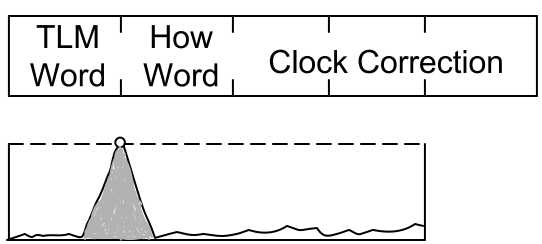
$(X_4 - U_X)^2 + (Y_4 - U_Y)^2 + (Z_4 - U_Z)^2 = (R_4 - C_B)^2$

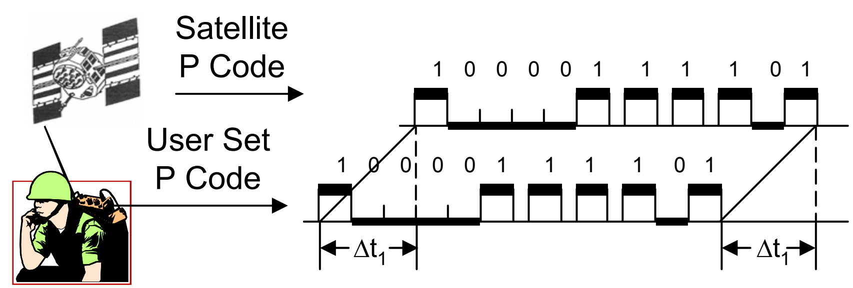
Acquiring the Military P(Y)-Code Signal

User-Set Matches the C/A Code



Strips off the Data - "How" Word Gives Address of P-Code Match





Pseudo Ranges:

$R_1 = C\Delta t_1$

$R_2 = C\Delta t_2$

$R_3 = C\Delta t_3$

$R_4 = C\Delta t_4$

Position Equations:

$$(X_1 - U_X)^2 + (Y_1 - U_Y)^2 + (Z_1 - U_Z)^2 = (R_1 - C_B)^2$$

$$(X_2 - U_X)^2 + (Y_2 - U_Y)^2 + (Z_2 - U_Z)^2 = (R_2 - C_B)^2$$

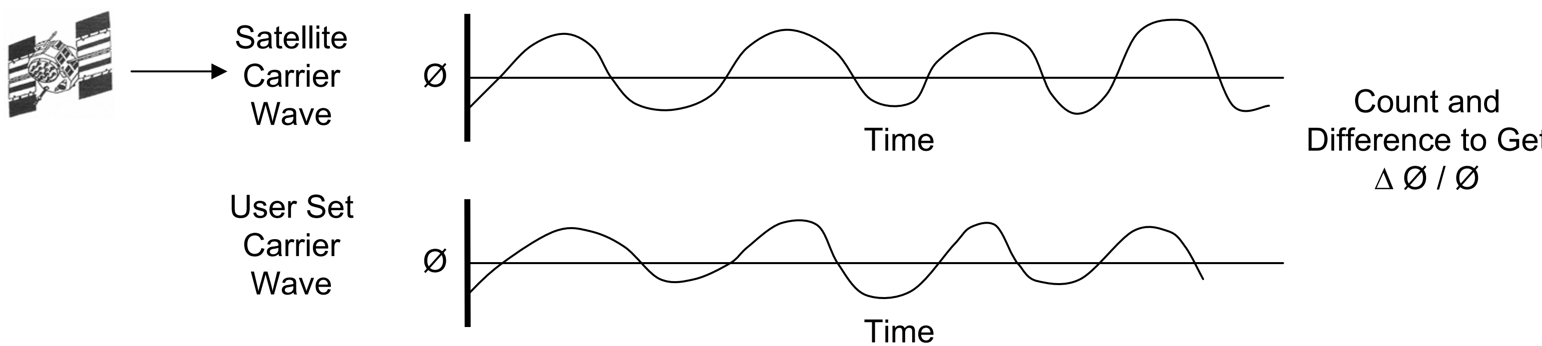
$$(X_3 - U_X)^2 + (Y_3 - U_Y)^2 + (Z_3 - U_Z)^2 = (R_3 - C_B)^2$$

$$(X_4 - U_X)^2 + (Y_4 - U_Y)^2 + (Z_4 - U_Z)^2 = (R_4 - C_B)^2$$

*C_B ~ 1/100 Sec for one week of user-set drift

Obtaining the Velocity Components

User-Set Locks onto Carrier to Obtain Doppler Shift

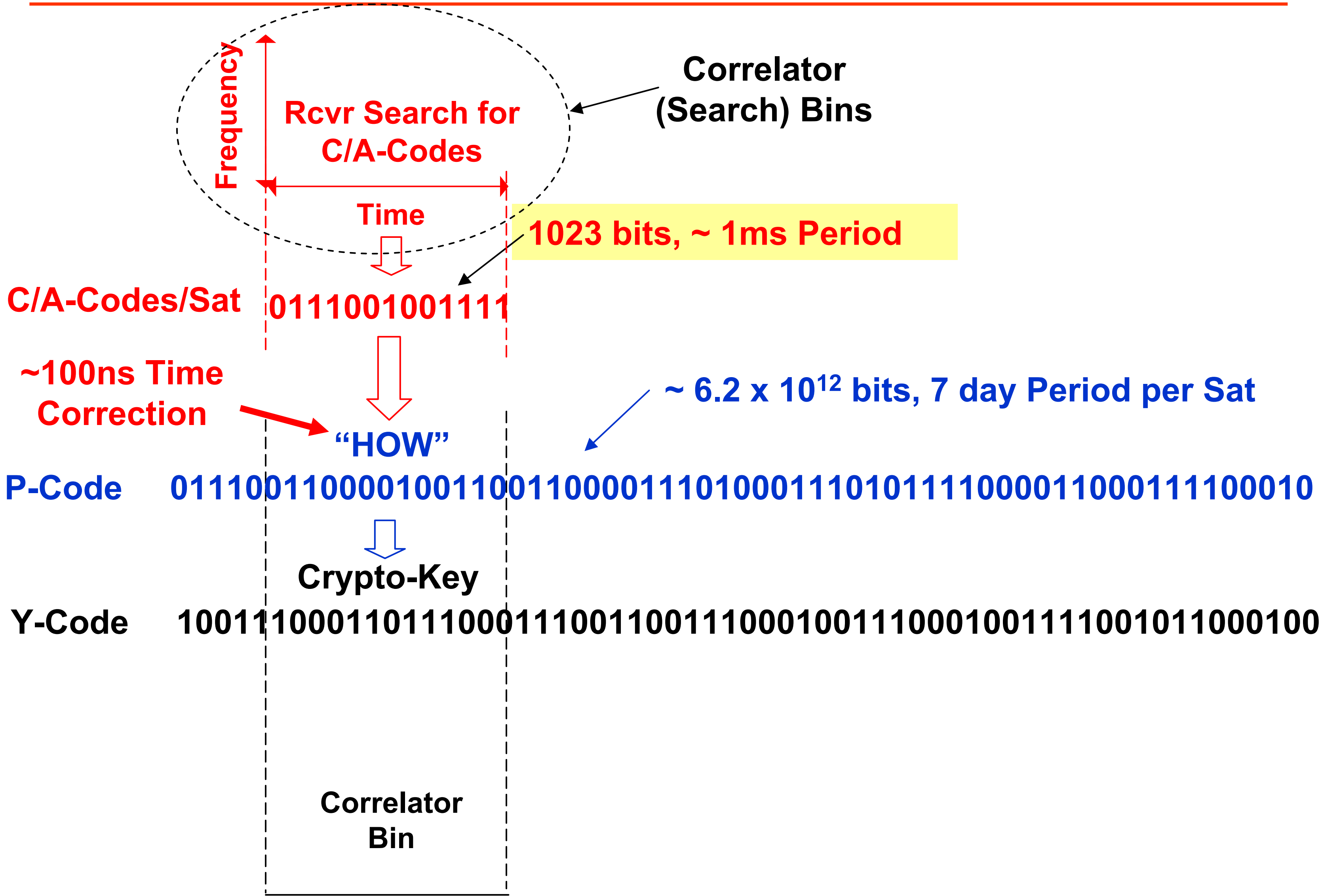


User-Set Performs the Navigation Solution for Velocity

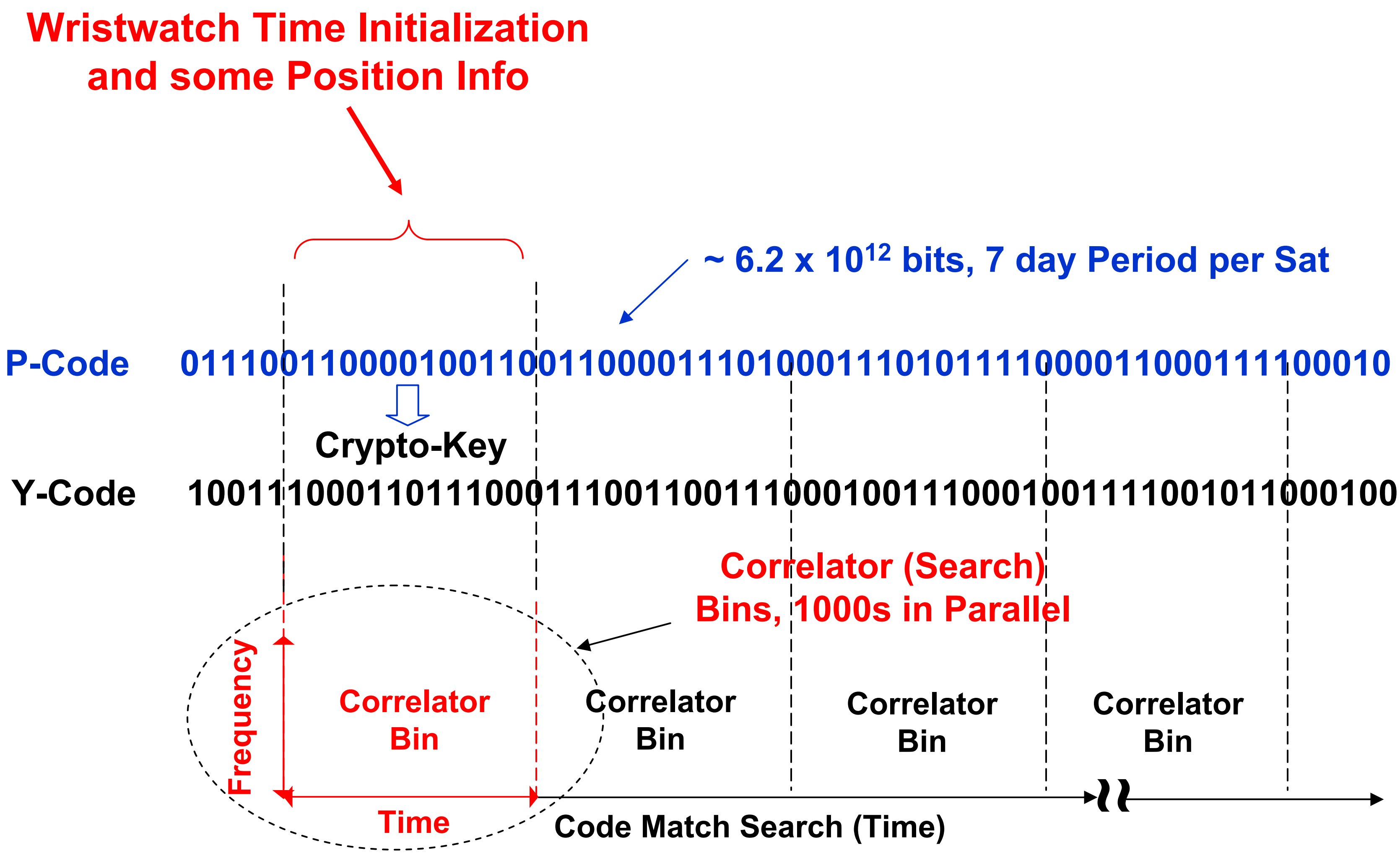
Range Rates:	Velocity Equations:
$\dot{R}_1 = \Delta \varnothing_1 / \varnothing_1 \, C$	$(X_1 - U_X)(\dot{X}_1 - \dot{U}_X) + (Y_1 - U_Y)(\dot{Y}_1 - \dot{U}_Y) + (Z_1 - U_Z)(\dot{Z}_1 - \dot{U}_Z) = R_1(\dot{R}_1 + \dot{C}_B)$
$\dot{R}_2 = \Delta \varnothing_2 / \varnothing_2 \, C$	$(X_2 - U_X)(\dot{X}_2 - \dot{U}_X) + (Y_2 - U_Y)(\dot{Y}_2 - \dot{U}_Y) + (Z_2 - U_Z)(\dot{Z}_2 - \dot{U}_Z) = R_2(\dot{R}_2 + \dot{C}_B)$
$\dot{R}_3 = \Delta \varnothing_3 / \varnothing_3 \, C$	$(X_3 - U_X)(\dot{X}_3 - \dot{U}_X) + (Y_3 - U_Y)(\dot{Y}_3 - \dot{U}_Y) + (Z_3 - U_Z)(\dot{Z}_3 - \dot{U}_Z) = R_3(\dot{R}_3 + \dot{C}_B)$
$\dot{R}_4 = \Delta \varnothing_4 / \varnothing_4 \, C$	$(X_4 - U_X)(\dot{X}_4 - \dot{U}_X) + (Y_4 - U_Y)(\dot{Y}_4 - \dot{U}_Y) + (Z_4 - U_Z)(\dot{Z}_4 - \dot{U}_Z) = R_4(\dot{R}_4 + \dot{C}_B)$

Where $\dot{C}_B$ = Frequency Drift in the User-Set Clock

Signal Acquisition - Conventional PPS RCVR



Signal Acquisition – Direct-P(Y) PPS RCVR



Typical Direct P(Y) Search Process Setup

1. ~1000 Parallel Correlators
   ÷ <u> 2.4 </u>Taps/Chip (ave.)
   ~ 420 Chips are searched

2. Setup of a 'Bin' depends on Time and Frequency Error

3. 'Bin' Time Error (horizontal axis)
   420 chips x ~100 ns per P-Code Chip
   = ~42μs per 'Bin'

4. 64 Tap FFT (64 Sections)

5. Typical 'coherent integration search time' per 'Bin' to meet 'Probability of Detection' goals is <u>5 ms</u>.

6. 'Bin' Freq. Error (vertical axis) = 0.5 x $\frac{1}{\text{search time}}$
   or 0.5 x $\frac{1}{5E-3}$ = 100 Hz per 'Bin'.
   So, total Freq. Error = 100 Hz x 64 sections
   = ± 3,200 Hz

5. Local oscillator frequency error generally rules over Doppler shift. A typical 0.25 to 1 ppm oscillator produces a frequency error at L1 of~ ±400 Hz to ±1,575 Hz.

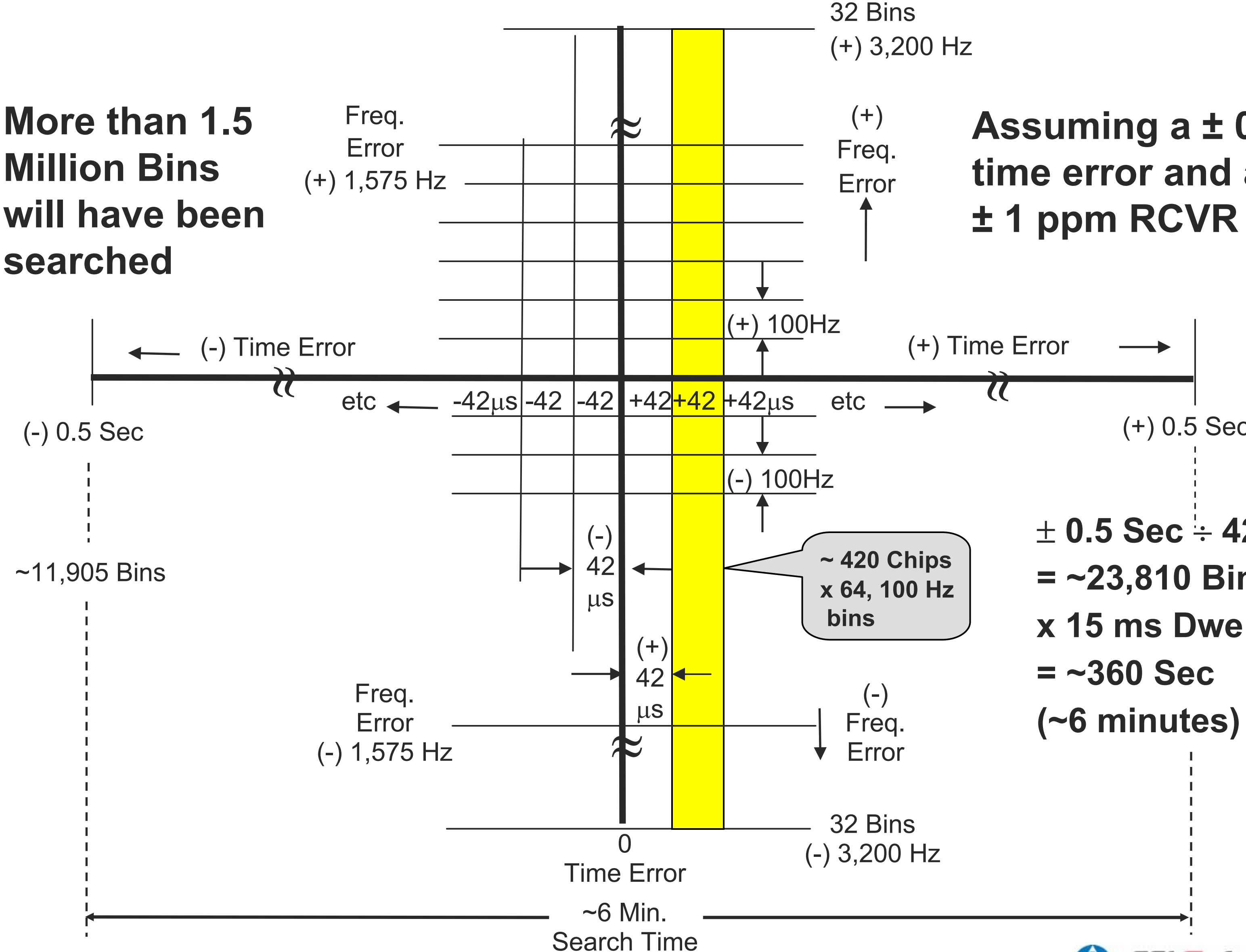
8. Depending on S/N, (3) 5 ms coherent searches may be required to meet 'probability of detection' goals. These are added non-coherently, = 15 ms search time per 'Bin'.

9. Typical example:
   - Assume ± 0.5 sec time error
   - Assume ± 1 ppm receiver clock
   - Assume (3) 5 ms dwells
   - Assume <u>No</u> jamming
   - Ideal Case

Rough example of a typical search process

More than 1.5 Million Bins will have been searched

Assuming a ± 0.5 sec time error and a ± 1 ppm RCVR clock



± 0.5 Sec ÷ 42 µs/Bin
= ~23,810 Bins
x 15 ms Dwell Time
= ~360 Sec
(~6 minutes)

Elements Involved in GPS Acquisition

External Factors

- Jamming or ambient noise level
- Signal blocking (canyons, buildings, trees, etc.)
- Civil (C/A) signal availability (level of SA, if on)
- Number of satellites in view
- Position of satellites (GDOP)
- Motion (and frequency of change) of GPS platform
- Velocity (Doppler) of GPS platform
- Vibration and Shock forces
- Initialization Parameters (Time and Position)

Internal Factors (RCVR)

- Acquisition sequence with C/A and P-Codes
- Signal Processing Architecture and Mfr's SW savvy
- Type of Key, if using PPS receiver
- Age of the ephemeris and Almanac
- Averaging Time of PVT Solutions
- RCVR noise level
- RCVR oscillator spec