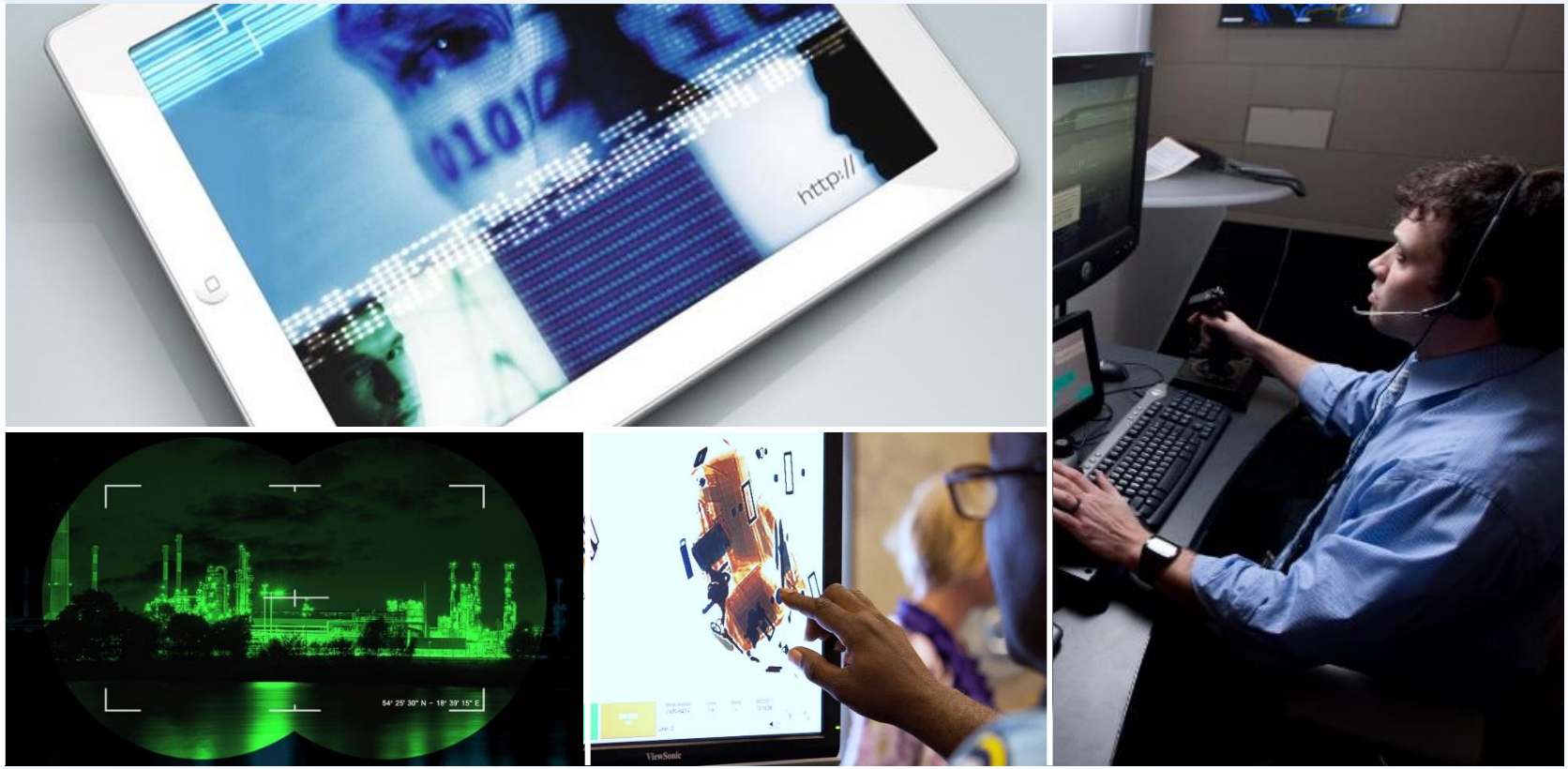
Responsible Use of GPS for Critical Infrastructure



Kevin M. Skey - skey@mitre.org

Homeland Security Systems Engineering and Development Institute

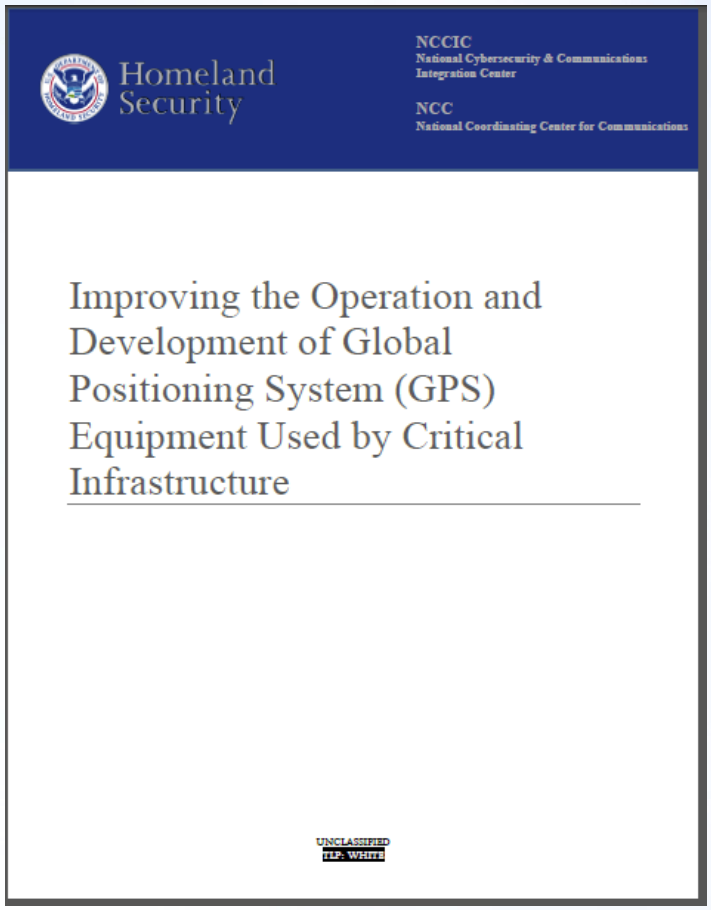
6 December 2017

HSSEDI
Homeland Security Systems Engineering and Development Institute

Introduction

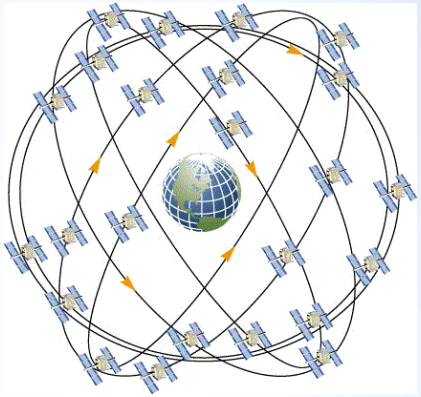
- **This discussion focuses on methods for increasing resilience of business operations reliant upon the civil GPS service by improving receivers and equipment installed in fixed infrastructure applications**
  - Based on DHS best practices recommendations

- **Generally, for…**
  - Receiver developers
  - Product and system integrators
  - End user

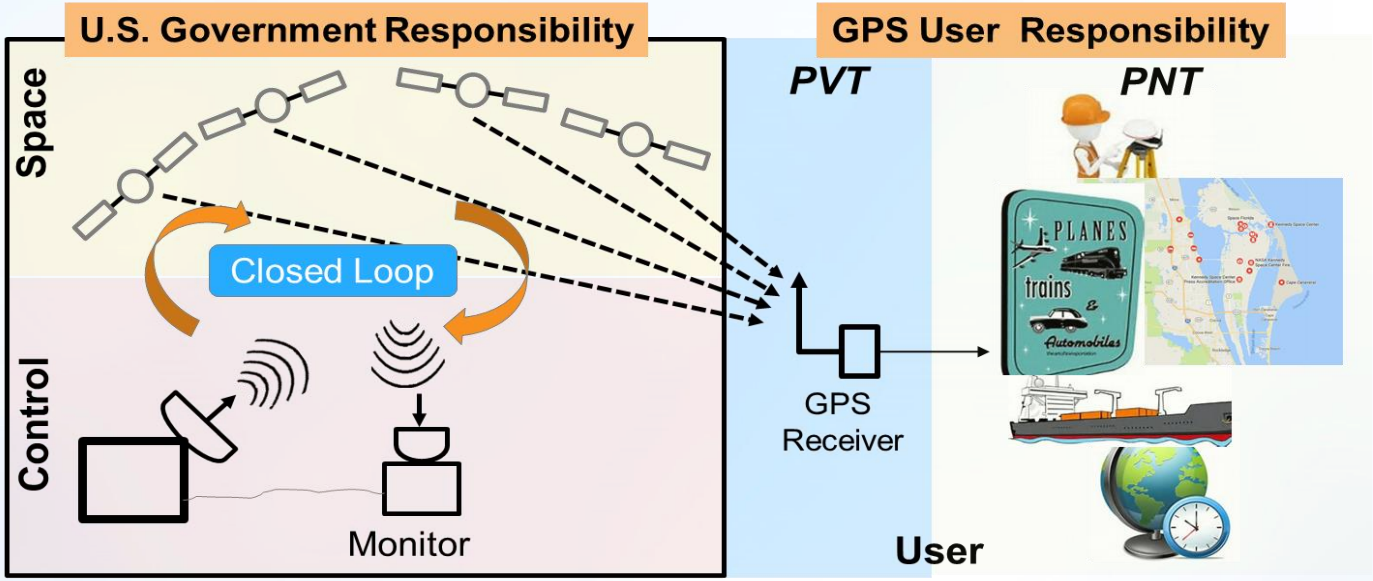


GPS System Overview

- **1 Nov 2017: 31 operating satellites with 35 in orbit**
  - 24 for baseline configuration
- **Orbital altitudes 20,200 km—medium earth orbit (MEO)**
- **4 open civil broadcast signals –** L1 C/A, L2C, L5, L1C
- **Satellites transmit navigation data (Ephemeris & Almanac) required for a receiver to calculate Position, Velocity and Time (PVT) –** The user decides how best to use PVT for Position, Navigation and Time **(PNT)**



https://www.gps.gov



GPS: The Good and The Bad

- **Civil GPS is the most ubiquitous, stable and highly adopted service for Position, Navigation and Time (PNT)**
  - Open signal broadcast -> **Free and No Authentication needed**
  - Open standard -> **Clear Understanding of System & Interoperability**
  - Efficient use of Spectrum -> **Single Freq, Power below the noise floor**
- **However, these positive attributes increase the fragility of a receiver making it susceptible to unintentional and intentional disruption**
  - It wasn't always this way…

How Did We Get Here for PNT?

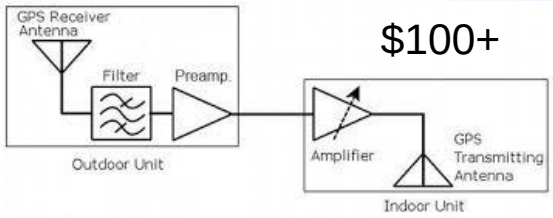
20th Century Perspective	21st Century Perspective
GPS is like the Internet-- wonderful technology, nice people	GPS is like the Internet-- wonderful technology, threats abound
GPS satellites are scarce, so receivers must be promiscuous	Since threats to GPS abound, so receivers must be robust and discriminating
GPS receivers are radios	GPS receivers are networked computers with a wireless access point

Need to Implement Best Practices -> Yielding 21st Century Equipment, Installations, and Operation to Address 21st Century Requirements and Threats

Threat Classes

- **Interference/jamming** - RF waveforms whose dominant effect is raise the effective noise floor in the receiver processing, denying, disrupting, or degrading the target receiver's ability to process desired signals
- **Measurement spoofing -** RF waveforms that mimic the true GPS signals to cause the target receiver to produce incorrect measurements of time of arrival or frequency of arrival or their rates of change
- **Data spoofing -** introduces incorrect digital data to the target receiver, for its use in processing of signals and the calculation of position, velocity, and time (PVT)
- **Effects -** can be instantaneous or delayed, and the effects can last as long as the spoofing is present, or longer.
- **Some attacks involve a combination of jamming and spoofing**

$500+



$100+

$1K+

$200K+

Approved for Public Release; Distribution Unlimited.
Case Number 17-4410 / DHS reference number 17-J-00100-01

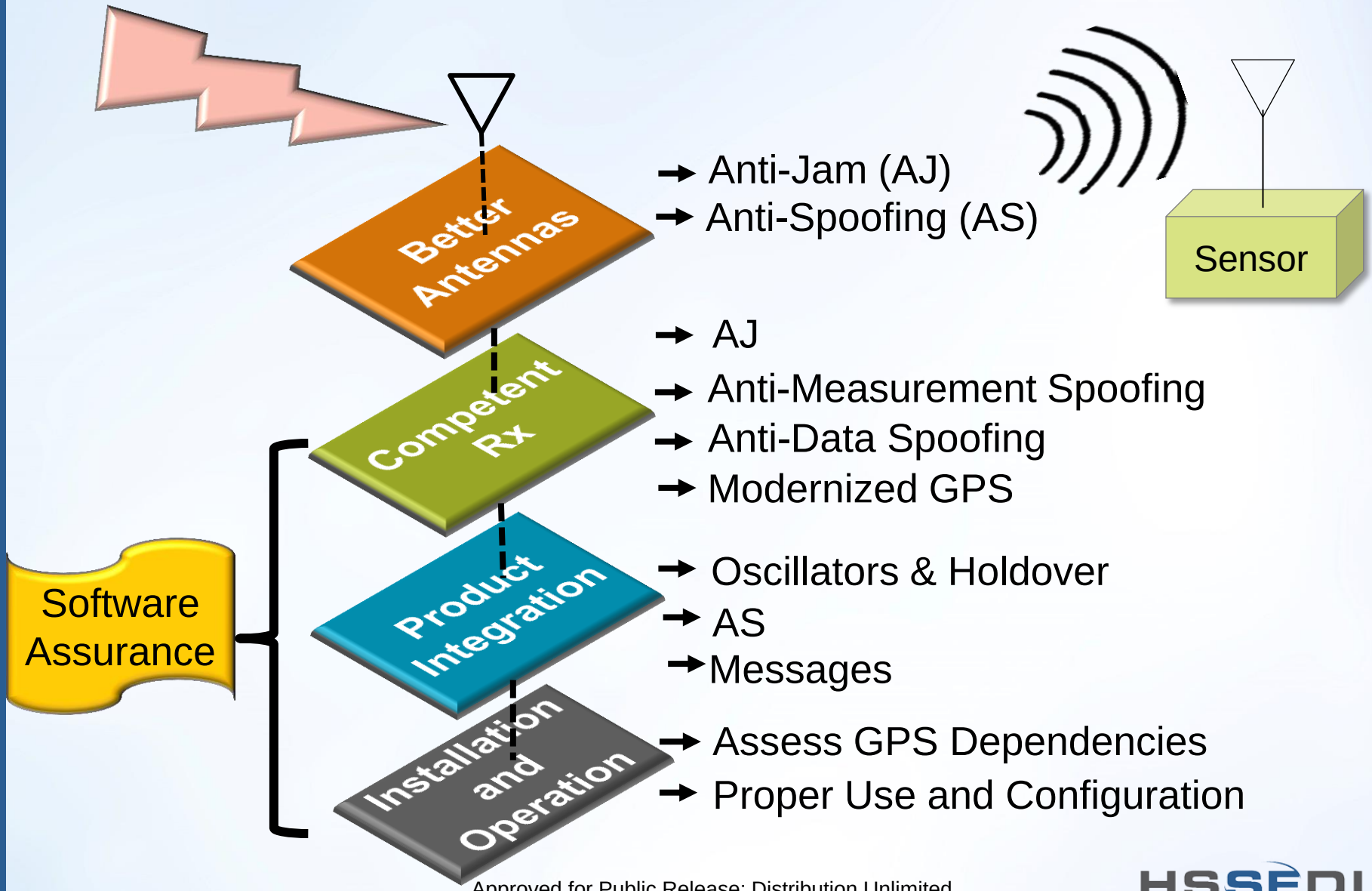
Need for Resiliency – Risk Management (RM)

- **From Presidential Policy Directive (PPD-21):** The term **"resilience"** means the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents

  https://www.dhs.gov/what-security-and-resilience

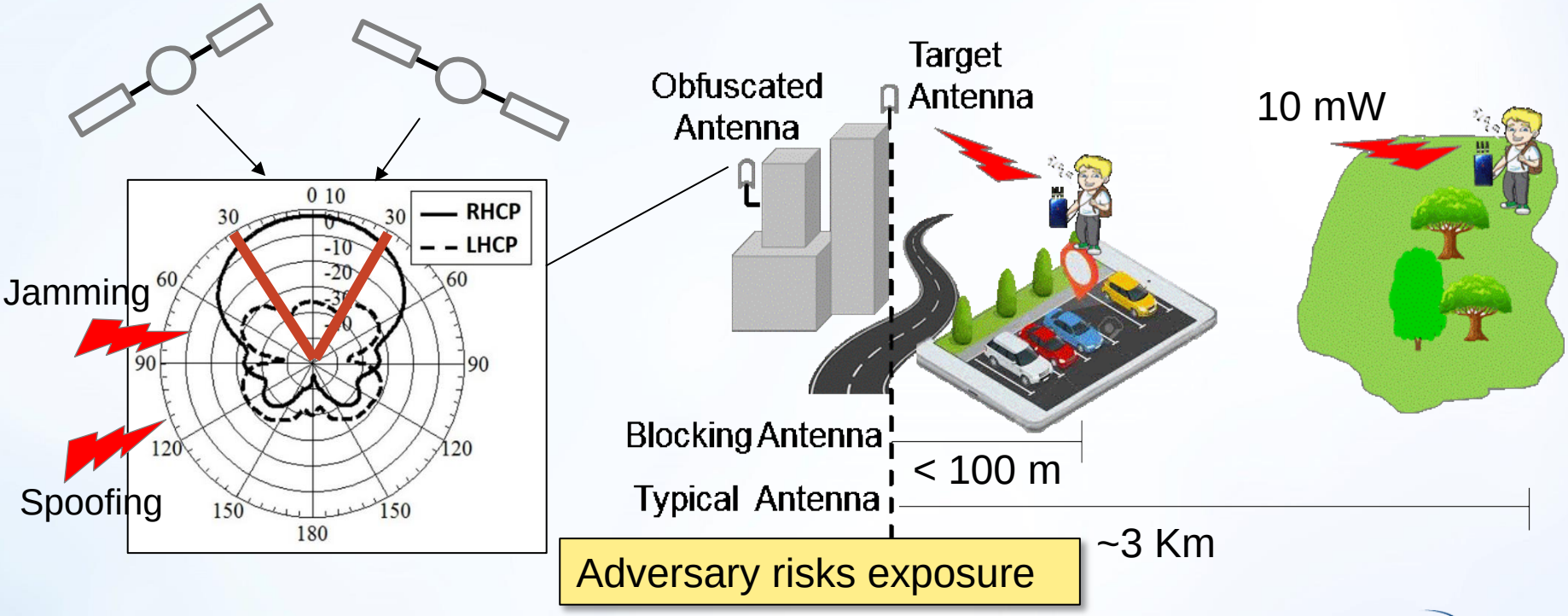
PPD-21 RM Examples	PNT Specific RM Examples
Developing a business continuity plan	Operations contingency planning – practices and procedures for GPS disruptions
Having a generator for back-up power	Alternate PNT sources – Clocks, inertial, GNSS, vision-aided, communication systems, RADAR, compass, etc.
Using building materials that are more durable	Antennas, protection algorithms, security engineering (IA), Cyber protections, adaptable system architectures

GPS Timing Receiver Defense-in-Depth Strategy



Blocking Antenna for Timing Applications

- **Threats assumed to be below antenna**
- **Blocking antenna reduces threat effectiveness by attenuating signals at or below horizon by > 30 dB with ~60° beam**
- **Forces adversary to either get closer or use bigger transmitter for more power**

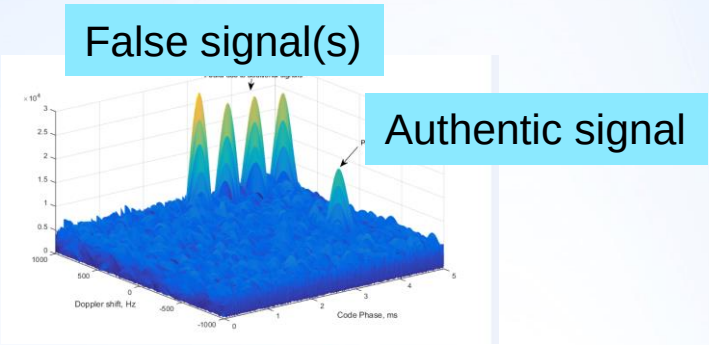


Competent Receiver: Enhanced Anti-Jam

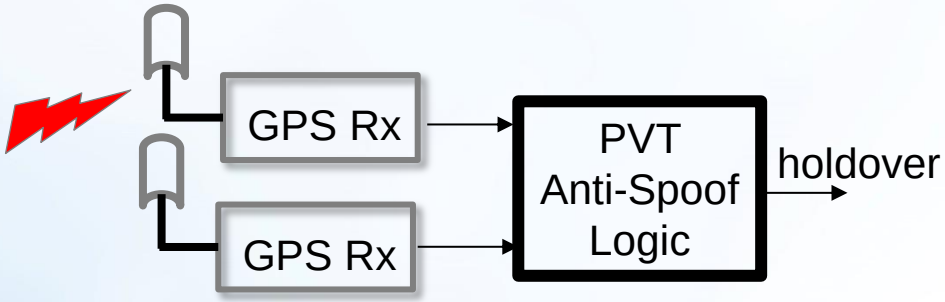
- **Interference and Jamming - most common threat to a GPS Rx**
  - In many cases, will appear as a raised noise floor
  - Prevents a GPS Rx from acquiring and tracking signals
- **Receiver developers should:**
  - Ensure analog filtering is adequate to reject out-of-band interference for unintentional events
  - Use enhanced digital filtering techniques for in-band interference/jamming
  - Use high sensitivity techniques for acquisition
  - Use robust tracking loop techniques applicable to stationary receivers
- **Receivers should also include monitoring for significant changes in RF power**
  - Can be an indicator of a spoofing attack as a false signal typically transmits a higher signal power than the GPS satellites

Competent Receiver: Anti-Measurement Spoofing

- **A receiver needs the ability to accurately discriminate between authentic and false signals**
  - Detection: repeater vs. signal generator
  - Mitigation: signal selection and denial
- **Multiple detectors should be implemented**
  - Detection algorithm type depends on access to receiver processing stage observables: Measurement, PVT
- **Mitigation for timing receiver can leverage clock holdover when GPS is declared to be invalid**

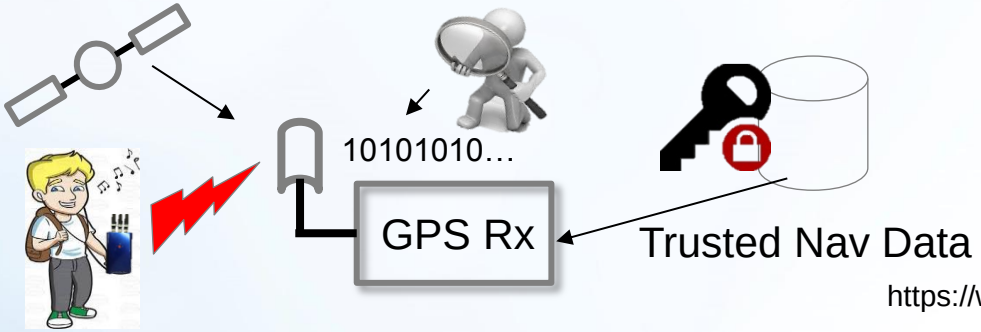


				Threat Class		
Category	Weight	Detector	Description	Interference/ Jamming	Measurement Spoofing	Data Spoofing
Receiver Detection	Med	AGC monitoring	Monitor the receiver's AGC level. If the AGC indicates additional power in band, it could be jamming or measurement anomaly	X	X	
	Med	C/N0 monitoring	A signal with too high of a C/N0 indicates possible measurement anomaly; All signals consistently low C/N0 indicates jamming;	X	X	
	High	Stationary position monitor	For stationary receivers the reported position should not deviate more than a pre-defined distance. If the position deviates, this may indicate measurement anomaly, but could also be multipath.		X	
	High	Dual antenna position monitor	Monitor for the difference in reported position by each of two receivers whose antennas are a fixed distance apart. If the difference decreases below a threshold (e.g. is zero) then a anomaly may be present.		X	
	Med	Stationary velocity monitor	For stationary receivers the expected speed is zero. If the reported velocity is significantly non-zero then a anomaly may be present.		X	
	Low	Clock bias and clock rate consistency	Clock rate and clock bias have an integral/derivative relationship. Monitor for inconsistencies in this relationship.		X	
	Low	Clock rate monitor	Monitors for large changes in clock rate measurement that exceed expectations of the receiver's local oscillator		X	



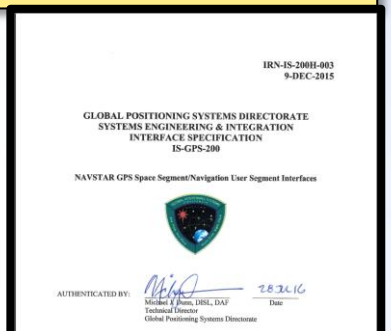
Competent Receiver: Anti-Data Spoofing

- **Data validation to protect Rx from processing intentional or unintentional GPS navigation (NAV) data broadcast errors**
  - January 25, 2016 event
  - Prevent writing bad data to memory
- **Whitelist method to validate known good data**
  - Inspect values, ranges, and temporal/state behaviors
  - Use secure network-based data services if possible
- **Validation rules should account for GPS system operational behaviors to prevent false alarms**
  - Test against historical databases and live sky



GPS ICD IRN-IS-200H-003 (RFC 268 – Data Message Validation Parameters and Clarifications) 28 Jul 2016

Added valid value ranges within the bit field


IRN-IS-200H-003
9-DEC-2015

GLOBAL POSITIONING SYSTEMS DIRECTORATE
SYSTEMS ENGINEERING & INTEGRATION
INTERFACE SPECIFICATION
IS-GPS-200

NAVSTAR GPS Space Segment/Navigation User Segment Interfaces

AUTHENTICATED BY:

TABLE 20-VI. ALMANAC PARAMETERS

Parameter	No. of Bits**	Scale Factor (LSB)	Valid Range***	Units
e	16	2^{-21}	0.0 to 0.03	dimensionless
t_{oa}	8	2^{12}	0 to 602,112	seconds
δ_i****	16*	2^{-19}		semi-circles
$\dot{\Omega}$	16*	2^{-38}	-6.33E-07 to 0	semi-circles/sec
$\sqrt{A}$	24	2^{-11}	2530 to 8192	$\sqrt{\text{meters}}$

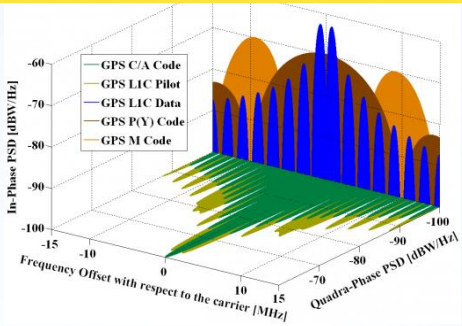
Ex: Limit range to LEO - HEO orbit heights.

https://www.gps.gov/technical/icwg/IRN-IS-200H-001+002+003_rollup.pdf

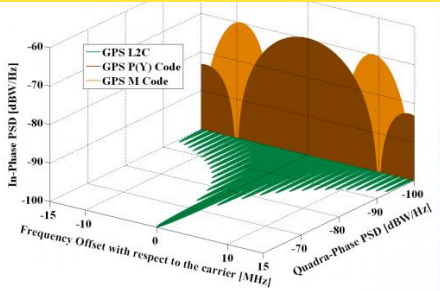
Competent Receiver: Use Modernized GPS

- **New GPS civil signals increase resiliency by adding both frequency and signal diversity**
  - L2C (19 SVs), L5 (12 SVs) and L1C (GPSIII Launch)
- **Improved signal structure - increased processing gain and upgraded message format**
  - Data-less pilot channel for L1C
  - Modernized CNAV is packet-based messages providing forward error correction (FEC) whereas L1 C/A LNAV is a fixed frame structure with simple CRC
- **More GPS signals enhances cross checks to aid in preventing measurement and data spoofing**

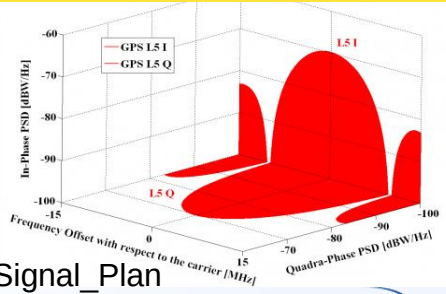
GPS L1 (1575.42 MHz)



GPS L2 (1227.60 MHz)



GPS L5 (1176.45 MHz)

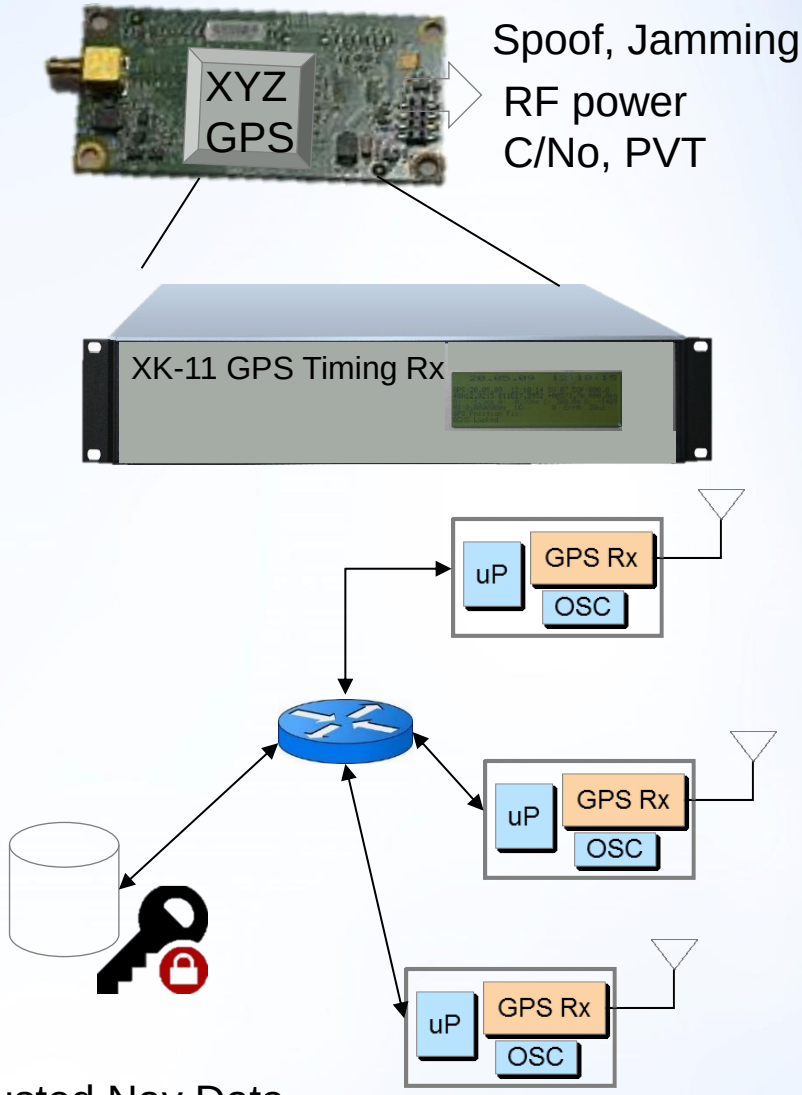


http://www.navipedia.net/index.php/GPS_Signal_Plan

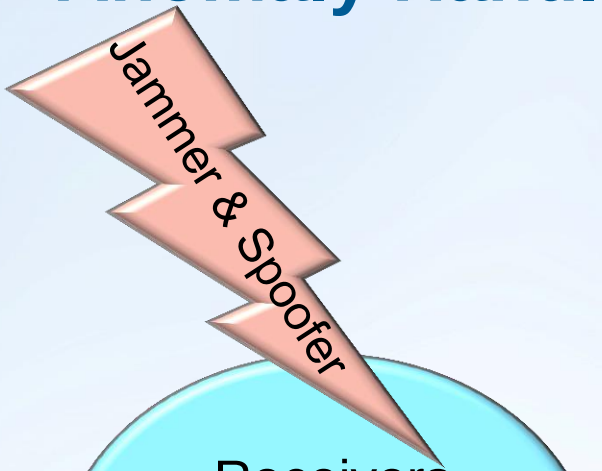
SV: Satellite Vehicle

Timing Receiver Product Integration

- **Timing receiver manufacturers should leverage OEM GPS Rx messages to develop detection and possibly mitigation capabilities**
  - Does it provide necessary observables for anomaly detection?
- **A capable GPS Rx should extend messages (or indicators) to measurement and data spoofing**
  - Enablers for alarms and holdover logic
- **Network capability should provide means to ingest known good navigation data and crosscheck voting**
- **Support for atomic clocks to meet stricter holdover requirements**



Anomaly Handling



Recognize

Anomalous Events

Report

Using Descriptive Messages
Inform Operators

Reject

False Signals
Illegal/Invalid Nav Data

Recover

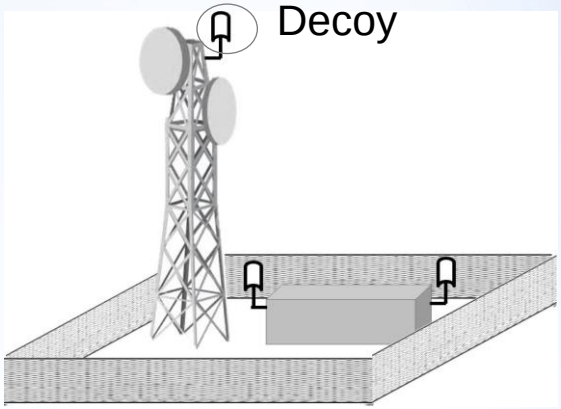
Graceful Error Handling
Return to Known Good State

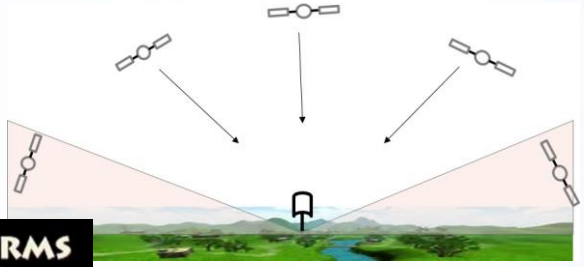
Eliminate erroneous outputs (e.g. position or time) which can impact dependent integrated systems

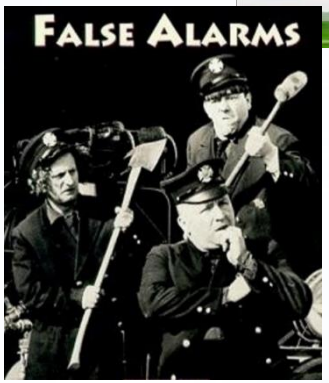
Operators should plan for localized long duration GPS outages

Timing Receiver Installation and Operation

- **First, why do you need GPS? Is it for convenience?**
  - NTP, PTP, holdover, wide area synchronization
- **Antenna considerations**
  - Performance: Blocking, Multipath mitigation
  - Security: Decoy, obfuscation
- **Redundant GPS Receivers**
  - More antennas + receivers – Crosscheck
- **Receiver capabilities and configuration**
  - Set elevation mask for low satellites
  - Use self survey and position hold
  - Understand the TRAIM algorithm
- **Datalogging and Alarms**
  - Loss of GPS, position jump, etc
  - Dropouts can be a normal occurrence

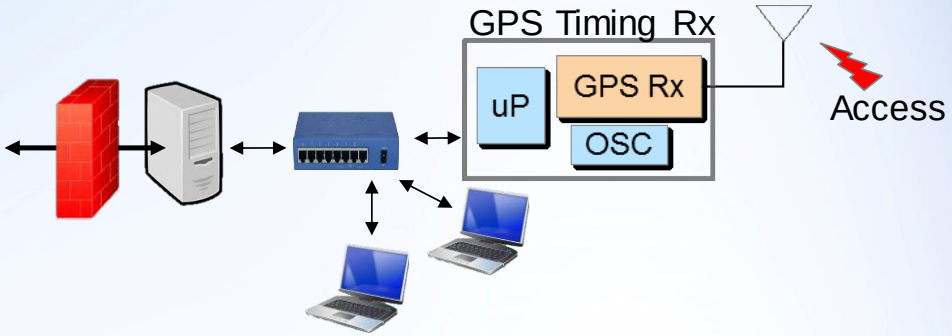




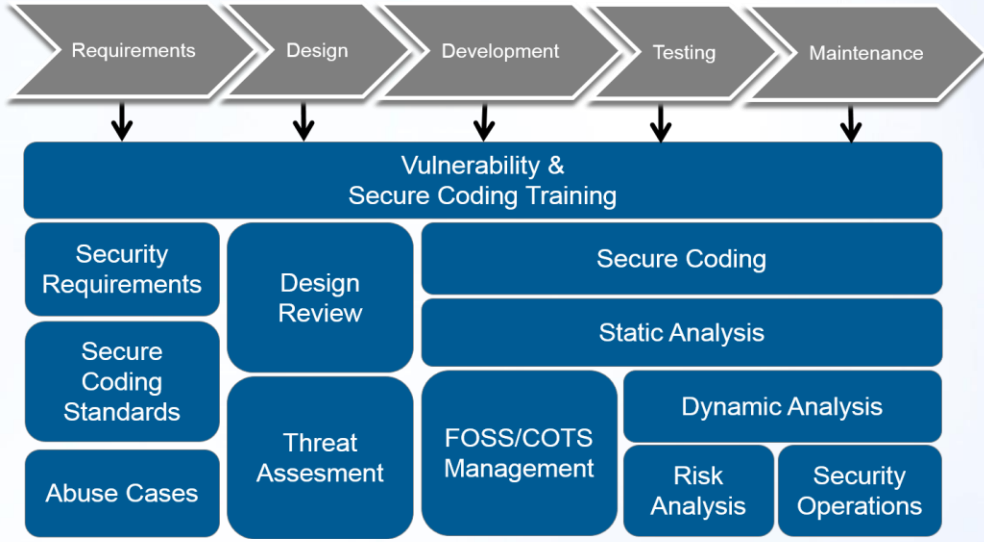


Software Assurance

- **GPS receivers are embedded computers that provide a wireless access point**
- **Product developers focus on functionality, secure coding is often left as an after thought**
  - Reliance on COTS and open source SW with unknown supply chain and non-vetted origins
- **Software assurance should be a standard part of the entire product life cycle including the embedded SW for the GPS Rx**
  - Development processes with analysis tools
  - Interface testing: Fuzz and Penetration



Software Development Life Cycle (Model Agnostic):
A Software Assurance Approach



GPS Week Rollover – April 6, 2019

- **GPS Week Number (WN) rolls to zero on April 6, 2019**
- **GPS WN field is 10 bits – every 1024 weeks it rolls to zero**
- **Receivers may not handle this rollover gracefully - causing Rx errors/failures and impacts to downstream systems**
- **Impacts many older receivers, less likely for newer receivers - however…**
- **"Trust but Verify"** - consult your manufacturer for any related product warnings and software patches
- **Conduct testing using GPS simulator**

TOKYO KEIKI

January 22 , 2014

Dear Customers

GPS Week Rollover Notice for Tokyo Keiki's GPS Products

Thank you very much for choosing our products.

As to the products, which has GPS receiver or the integrated system, GPS week rollover[1] issues may occur and indicate previous date after the date specified in the table below. (The occurrence date of rollover varies and depends on the design of GPS.)
However, the time and the positioning other than the date will operate in normal.

Once the rollover occurs, date will go back 1,024 weeks and the system will output the previous date as well. If some equipment or system utilize the ZDA[2] sentence from our GPS Products just for other than date-display, they may generate a false alarm for the above reason.

We stopped the production of all the Tokyo Keiki products except for TRA-2000 in the table below for more than 10 years. And we are forced to discontinue their maintenance due to various reasons. Therefore in

NovAtel

February 10, 2017 — NovAtel Service Bulletin — Page 1 of 1

WAAS GUS Type-I Receiver 2019 GPS Week Rollover

Summary:
On April 7 2019, the GPS week number that is broadcast as part of the GPS message will roll over from 1023 to 0. Affected units will stop tracking all satellites until the system is reset.

Products Affected:
- WAAS GUS-Type 1

Affected Firmware Versions:
- WAAS firmware version x.104 or x.105 and all previous versions are affected.
- EGNOS firmware versions x.110A1 or x.110 and all previous versions are affected.

Details:
The GPS week number count began at 0 on January 5 1980, incrementing by one every week. At the completion of week 1023, the count rolls over to 0. The next week rollover will occur on April 7 2019. Current versions of the GUS-Type 1 WAAS and EGNOS firmware will stop tracking at the week rollover. Resetting the receiver after the event will restore normal operation.

Solution:
An unqualified Alpha version of software is available for both WAAS and EGNOS versions of the firmware that allows the product to operate correctly through the week rollover event. A fully qualified release version of software is expected to be available June 2017.

Contact Information:
For any questions or to obtain Alpha firmware for evaluation, please contact:

Allan MacAulay
Business Development Manager, Safety Critical Systems
allan.macaulay@novatel.com

Useful Reference Products

Protection	Reference	Available	Contact
Blocking Antenna	HSSEDI Total Horizon Antenna Reference Design	Now	MITRE TTO
Anti-Measurement Spoof detection	HSSEDI PVT-based spoof detection algorithms	Jan 2018	MITRE TTO
Anti-Data Spoofing	IS-GPS-200H	Now	https://www.gps.gov/technical/icwg/IRN-IS-200H-001+002+003_rollup.pdf
Power Detection	HSSEDI Interference detection mitigation applique (GIDMA)	Now	MITRE TTO
Threat Environment recordings	Recording from DHS GET-CI Sept 2017	Mar 2018	Keith Connor, DHS S&T PNT

MITRE Technology Transfer Office (TTO):
Barry Costa: bac@mitre.org
Poornima Deshpande: poornima@mitre.org

Conclusion

- **GPS receivers can be made much less susceptible to jamming and spoofing**
- **Even with emerging threats, the GPS benefits still outweigh the risk given appropriate measures are taken**
  - Robust timing receivers and related protection devices are beginning to appear on the market
- **Determine if your system requires GPS for accuracy and/or system synchronization**
  - Don't unintentionally introduce a potential access vulnerability
- **If using GPS, understand your system dependences - what happens if GPS drops out? Provides a bad output e.g. time/date? How long can you operate without it?**
- **Accept that the threat is not going away - use industry best practices for the design, installation and operation of GPS-based timing sources**

Approved for Public Release; Distribution Unlimited.
Case Number 17-4410 / DHS reference number 17-J-00100-01