sponsored by

InsideGNSS
GPS | GALILEO | GLONASS | BEIDOU

NovAtel

inside
unmanned systems

NOISES OFF:
GNSS INTERFERENCE AND MITIGATION TECHNIQUES

May 25, 2016

WELCOME TO

Noises Off:

GNSS Interference and Mitigation Techniques

Guy Buesnel
CPhys, FRIN
Spirent

Rick Hamilton
U.S. Coast Guard Navigation Center

Grace Gao
Asst. Professor Aerospace Engineering University of Illinois Urbana-Champaign

Co-Moderator: Lori Dearman, Sr. Webinar Producer

Who's In the Audience?

A diverse audience of over 500 GNSS and unmanned professionals registered from 58 countries, 36 states and provinces representing the following categories:

19% GNSS Equipment Manufacturer

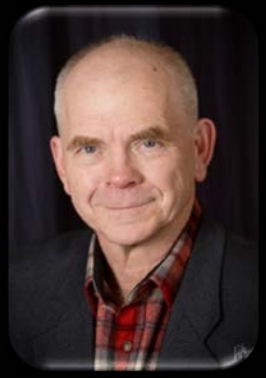
17% Professional User

16% Product/Application Designer

15% System Integrator

33% Other

Welcome from *Inside GNSS*



Glen Gibbons

Editor and Publisher
Inside GNSS

Demoz Gebre-Egziabher
Aerospace Engineer and
Mechanics Faculty
University of Minnesota

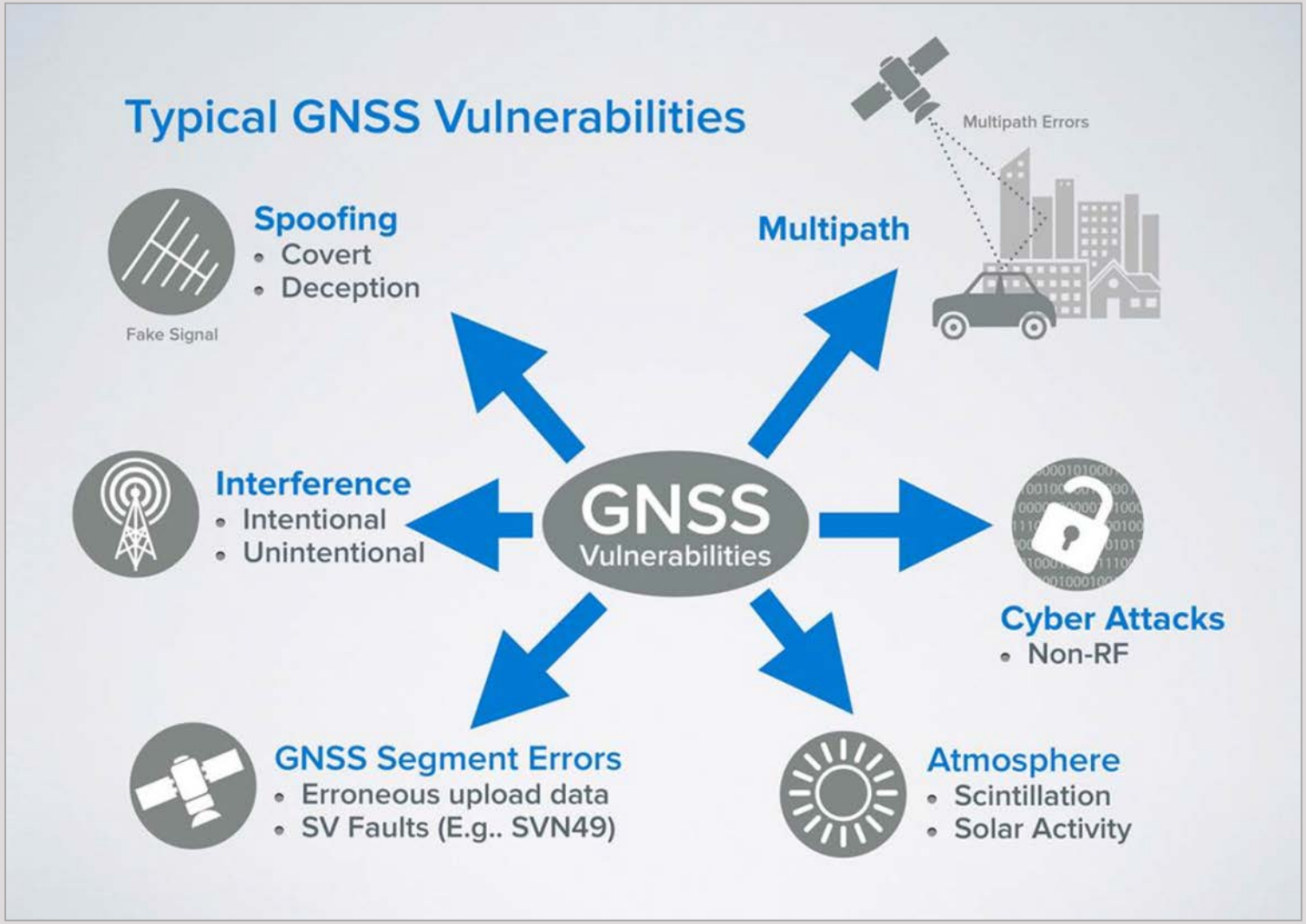
Poll #1

With the ubiquity of GPS and our increased reliance on it, jamming and interference incidents:

a. Are becoming rare due to increased awareness.
b. Are becoming more frequent and worse.
c. Occur at the same frequency (we are just more aware of them now).
d. Phft! A non-issue for new receiver designs!

Risk Assessment of GNSS Interference

Guy Buesnel
CPhys, FRIN
Spirent


Typical GNSS Vulnerabilities
Multipath Errors
Spoofing
• Covert
• Deception
Fake Signal
Multipath
Interference
• Intentional
• Unintentional
GNSS
Vulnerabilities
Cyber Attacks
• Non-RF
GNSS Segment Errors
• Erroneous upload data
• SV Faults (E.g.. SVN49)
Atmosphere
• Scintillation
• Solar Activity

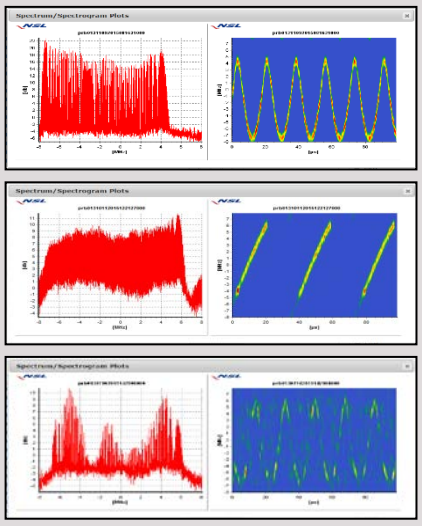
How likely is it that GNSS systems could be disrupted?

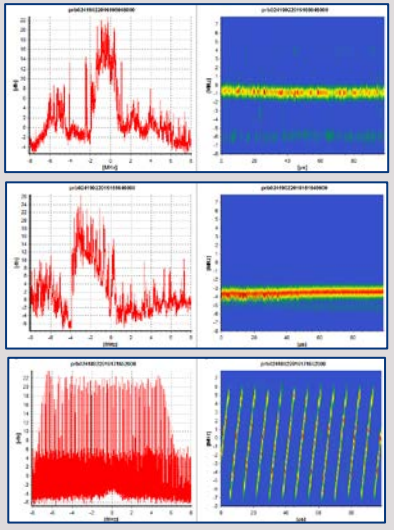
Spirent Paignton, UK

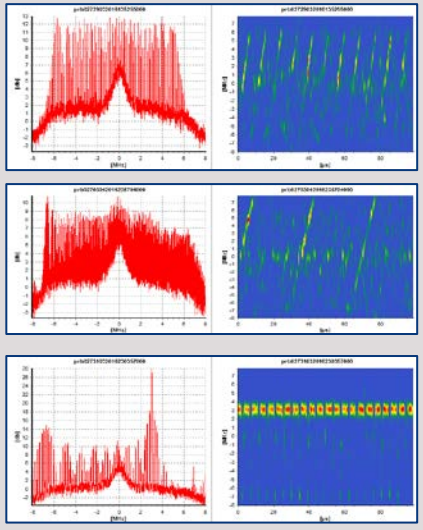
European Airport

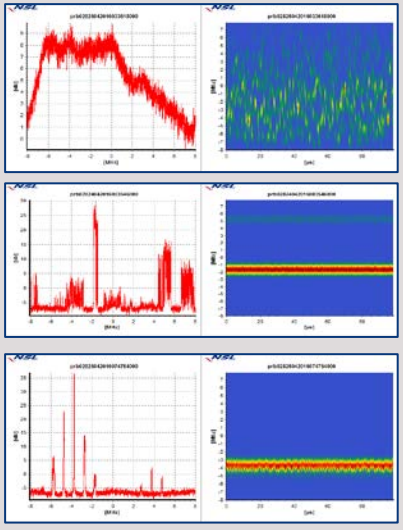
Spirent San Jose, US

AmTechs, JAPAN







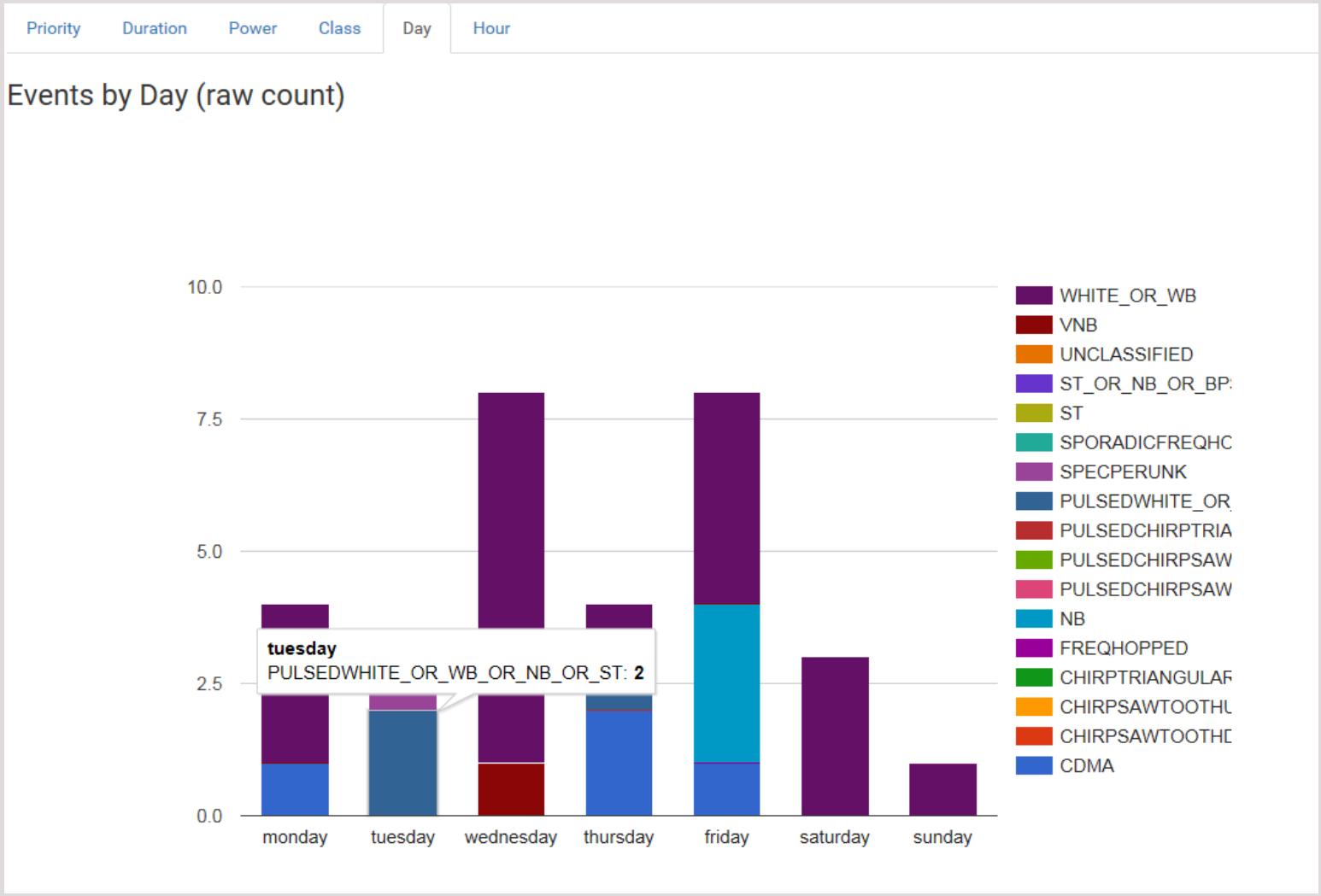


How likely is it that GNSS systems could be disrupted?

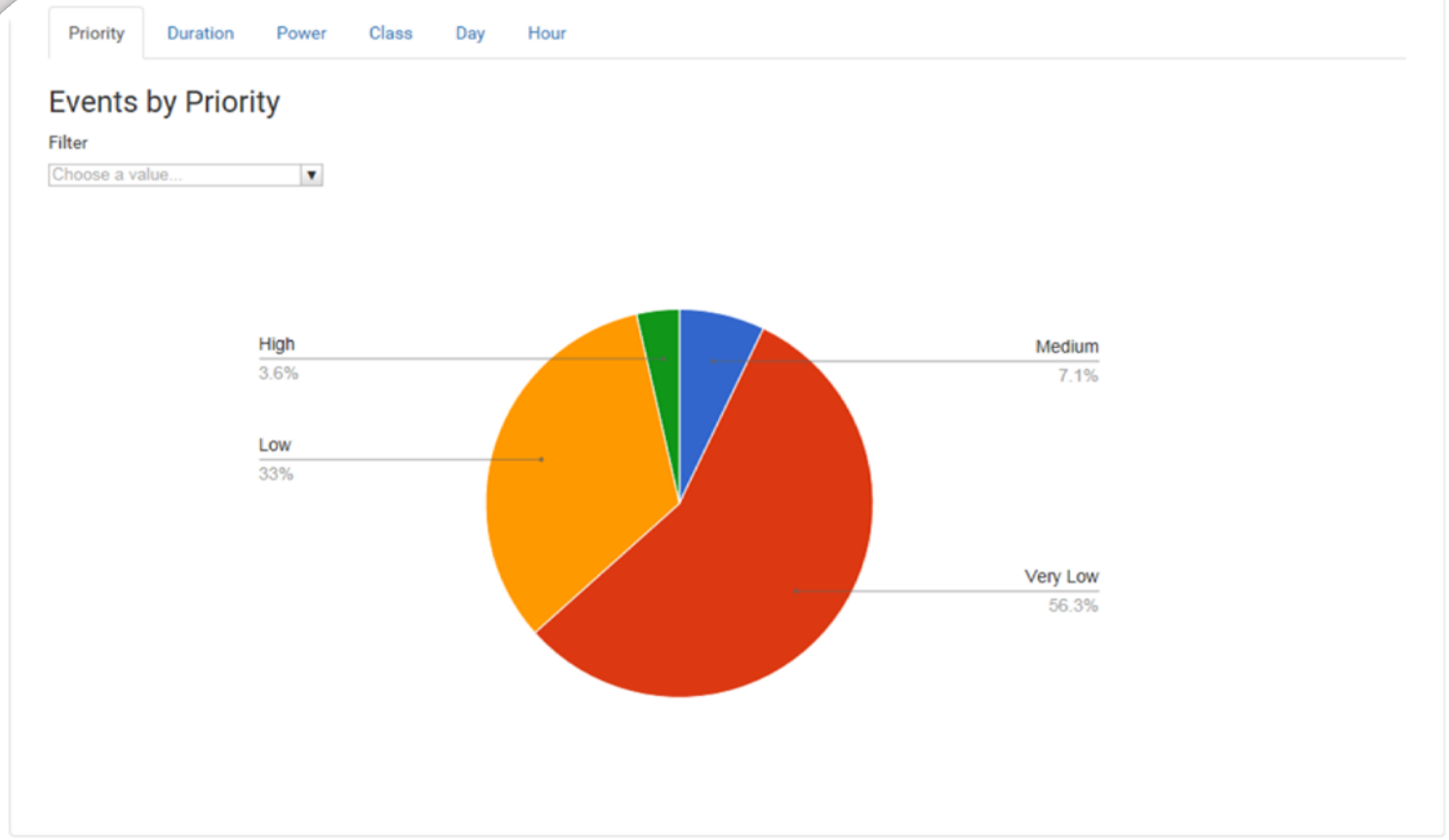
Spirent San Jose, US

Event ID	Event Priority	Detector	Event Start Time	Duration (secs)	Event Type	Event Class	Max Power
188	Very Low	PRB027	2016-05-06 13:37:39	10	Automatic_Detection	WHITE_OR_WB	1.9949
185	Low	PRB027	2016-05-06 05:41:16	20	Automatic_Detection	CDMA	2.0481
183	Low	PRB027	2016-05-06 01:06:47	26	Automatic_Detection	NB	2.3071
179	Low	PRB027	2016-05-05 21:31:14	10	Automatic_Detection	PULSEDWHITE_OR_WB_OR_NB_OR_ST	2.3961
177	Low	PRB027	2016-05-05 14:55:11	10	Automatic_Detection	WHITE_OR_WB	2.0469
169	Very Low	PRB027	2016-05-04 21:21:00	16	Automatic_Detection	WHITE_OR_WB	1.8914
165	Low	PRB027	2016-05-04 16:32:00	10	Automatic_Detection	VNB	2.2271
144	Low	PRB027	2016-05-04 12:53:04	10	Automatic_Detection	WHITE_OR_WB	2.0291
138	Very Low	PRB027	2016-05-04 05:34:47	19	Automatic_Detection	WHITE_OR_WB	1.9741
136	Low	PRB027	2016-05-03 23:29:32	10	Automatic_Detection	SPECPERUNK	2.0153
Event ID	Event Priority	Detector	Event Start Time	Duration (secs)	Event Type	Event Class	Max Power

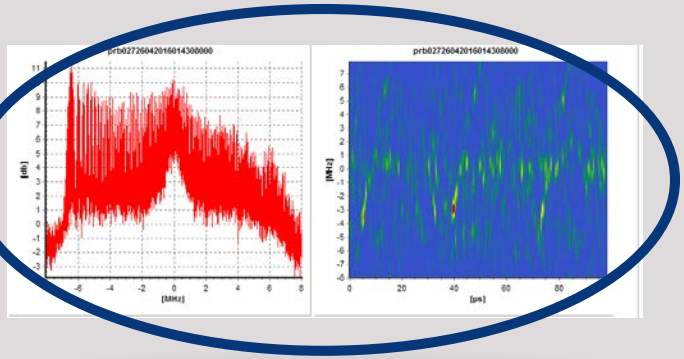
How likely is it that GNSS systems could be disrupted?

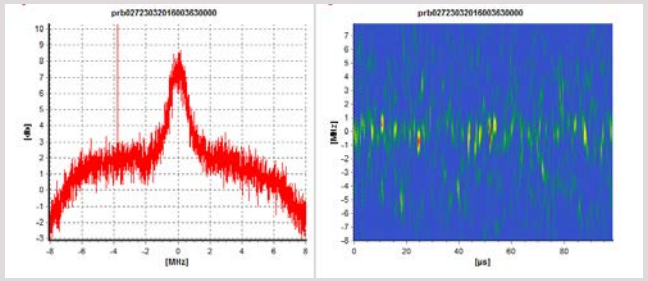


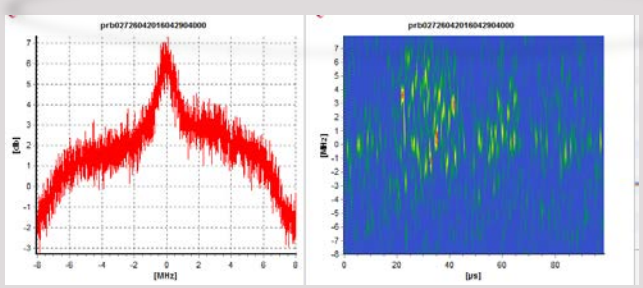
How likely is it that GNSS systems could be disrupted?

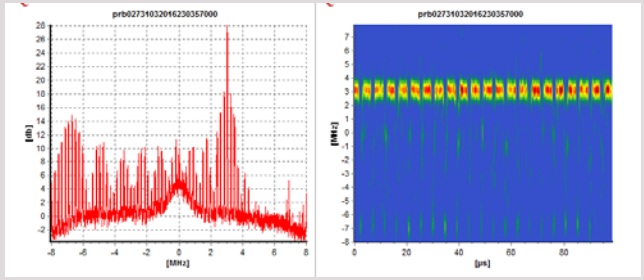


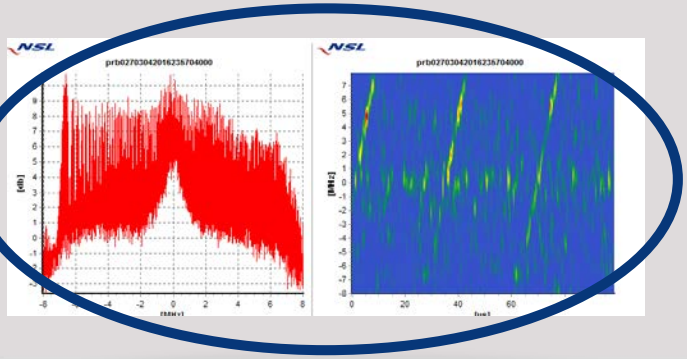
Some of the events detected in San Jose 2016….

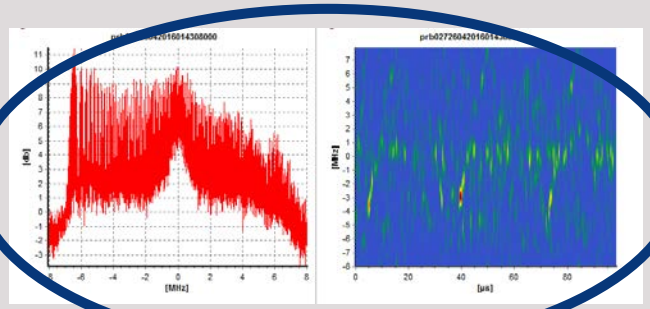




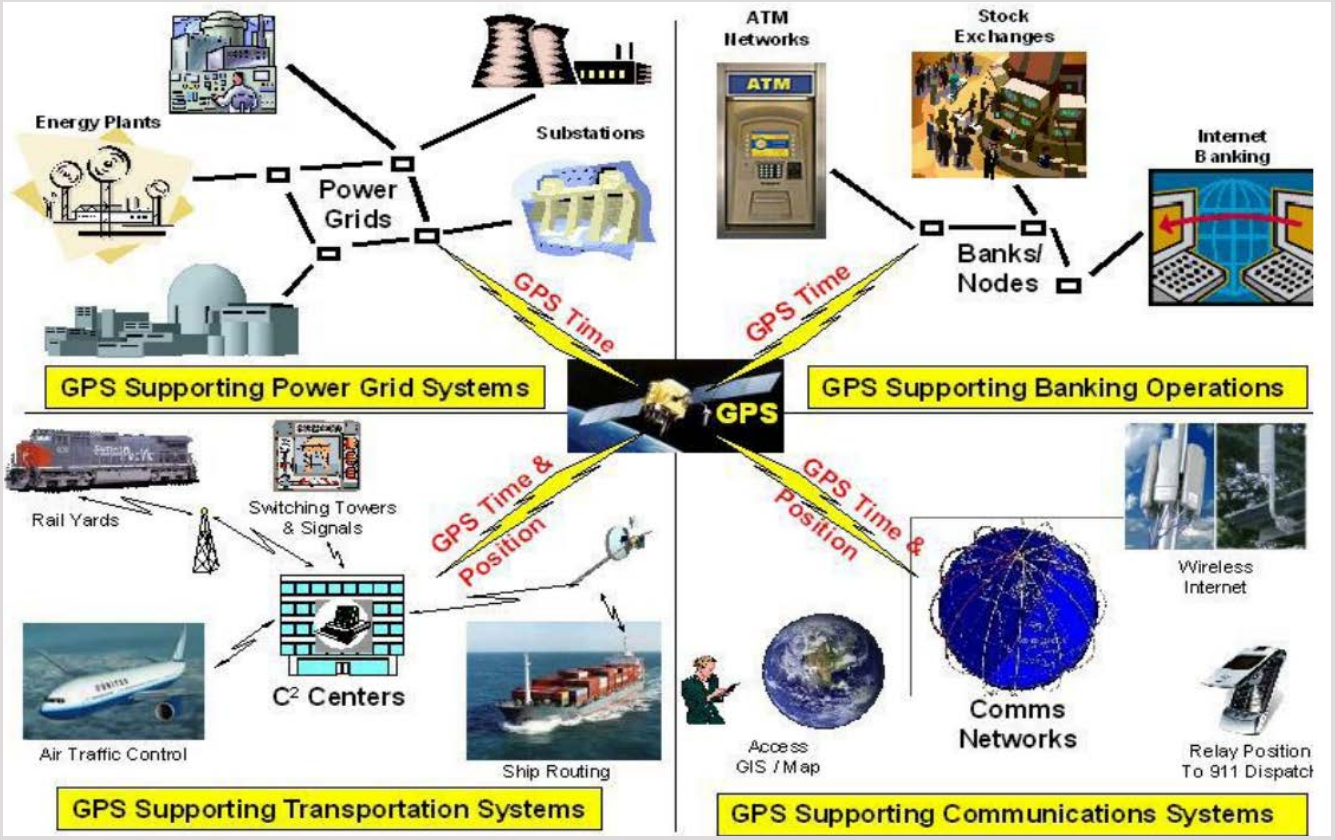








- **US Department of Homeland Security**
  "15 of the 19 Critical Infrastructure & Key Resources Sectors have some degree of GPS timing usage"



Source: http://www.gps.gov/multimedia/presentations/2012/10/USTTI

GPS Jamming – real cases

"This past summer, multiple outbound vessels from a non-U.S. port suddenly lost GPS signal reception. The net effect was various alarms and a loss of GPS input to the ship's surface search radar, gyro units and Electronic Chart Display & Information System (ECDIS), resulting in no GPS data for position fixing, radar over ground speed inputs, gyro speed input and loss of collision avoidance capabilities on the radar display."

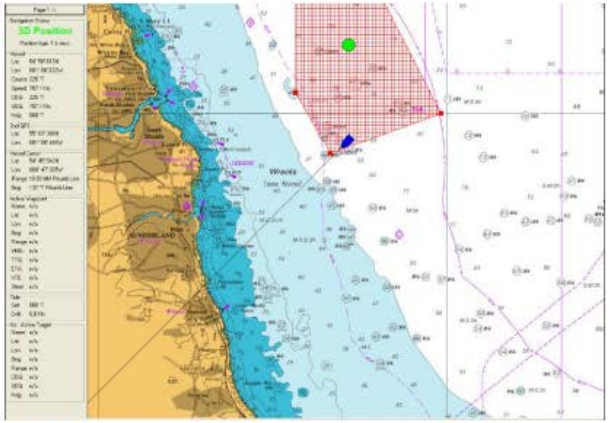
These types of events highlight the potential detrimental impact to navigation caused by GPS interference or jamming and the importance in understanding how your vessel's or facility's equipment could be impacted by a loss of GPS signal."

Source: http://www.gps.gov/news/ &
http://www.uscg.mil/hq/cg5/cg545/alerts/0116.pdf

GLA GPS Jamming trial 2010

RESEARCH & RADIONAVIGATION
GENERAL LIGHTHOUSE AUTHORITIES
United Kingdom and Ireland

With low power jammer on board...



Jammer of less than 1 milliWatt:

- **False positions, and velocities**
- **Autopilot may turn vessel**
- **But no alarms!**

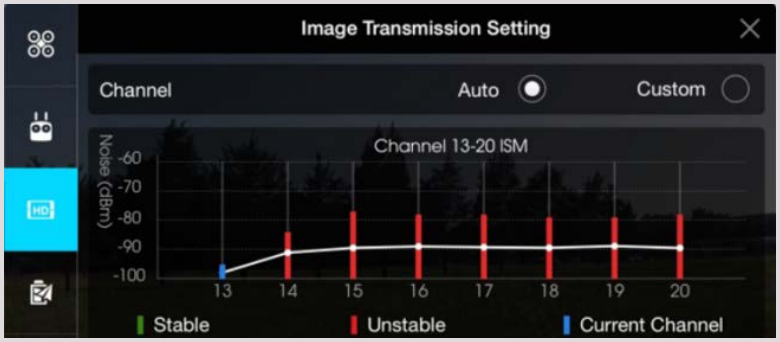
Hazardously Misleading Information

With a little more jammer power:

- **Electronic Chart Displays**
- **Autopilot**
- **Automatic Identification System**
- **Differential GPS**
- **Satellite voice and data comms**
- **Maritime distress safety system**
- **Ship's radar & gyrocompass**

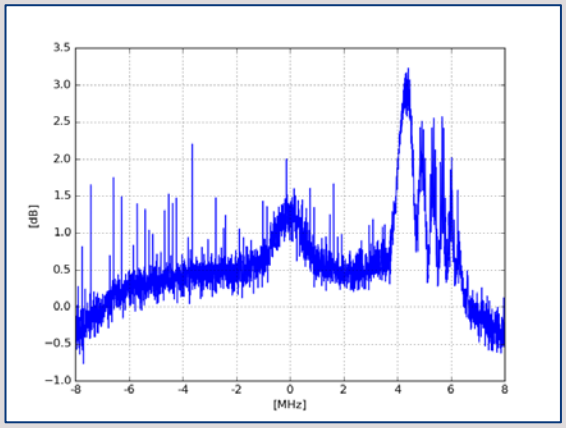
Source: GLA, UK

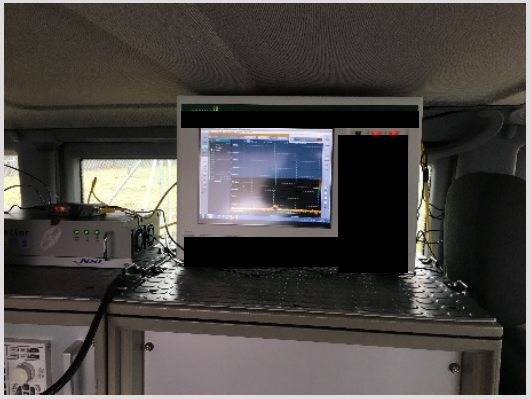
- Michael Robinson–DEFCON 23, August 2015
  - *"Knocking my Neighbor's Kid's cruddy drone offline"*



- Demonstrating the effect of disrupted (jammed) GPS Signal on a flying drone…
  - The Video feed started to jitter and video feeds were tagged as "unstable"
    - Video synch using precise timing from GPS

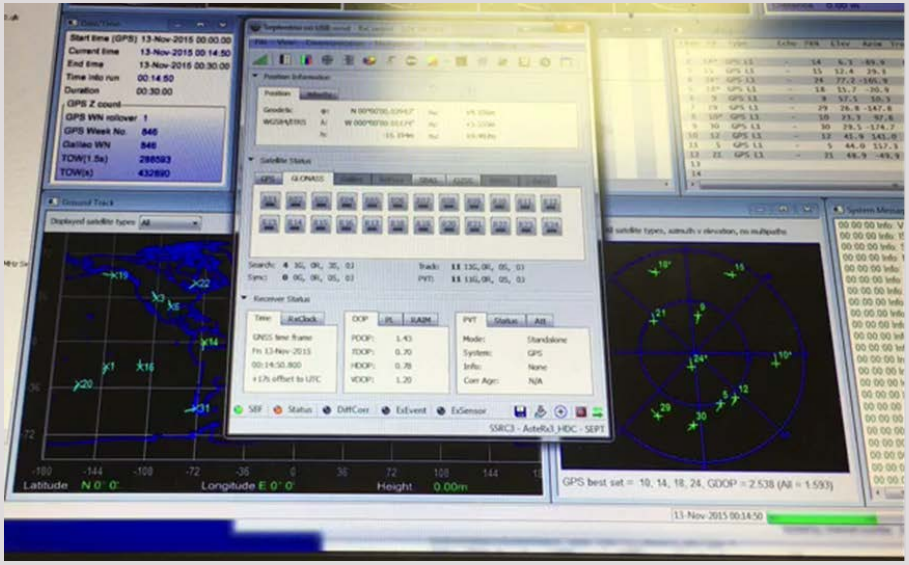
GPS Interference may cause unexpected behaviour in an unprotected system



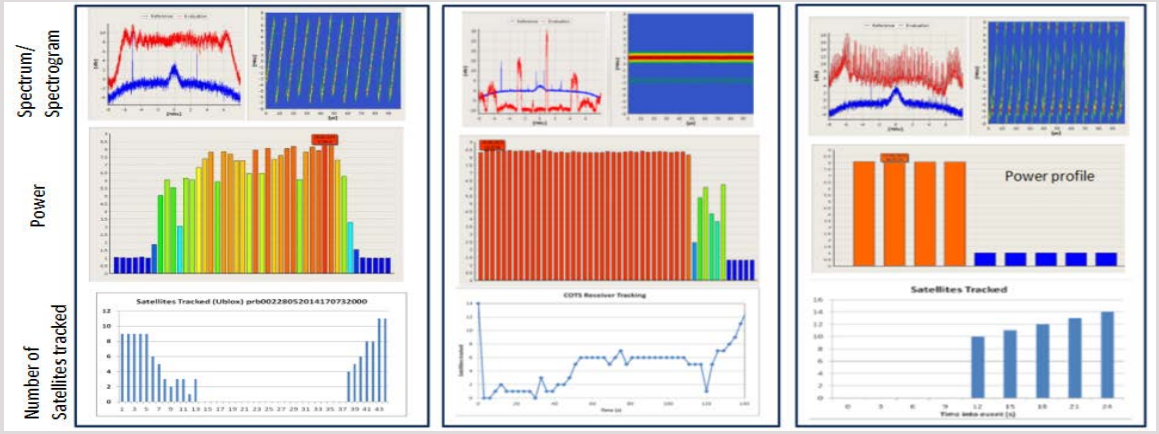


- Detected interference event correlated with compromise of ICAO interference mask profile

Scenario:
Moving Jammer on Fixed GPS RX Location



- Jammer Signal is moving relative to GPS RX location
- Max Jammer power is 13dBm at 10m from GPS RX location.
- Scenario ramps -140dBm to -40dBm power
- Varying jammer signals including Saw Tooth, Triangular and Sinusoid Chirp sweeps
- Can include real events captured from jamming Detectors

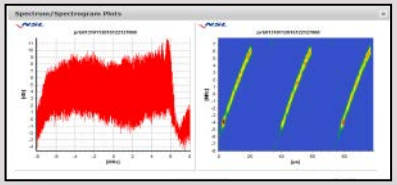


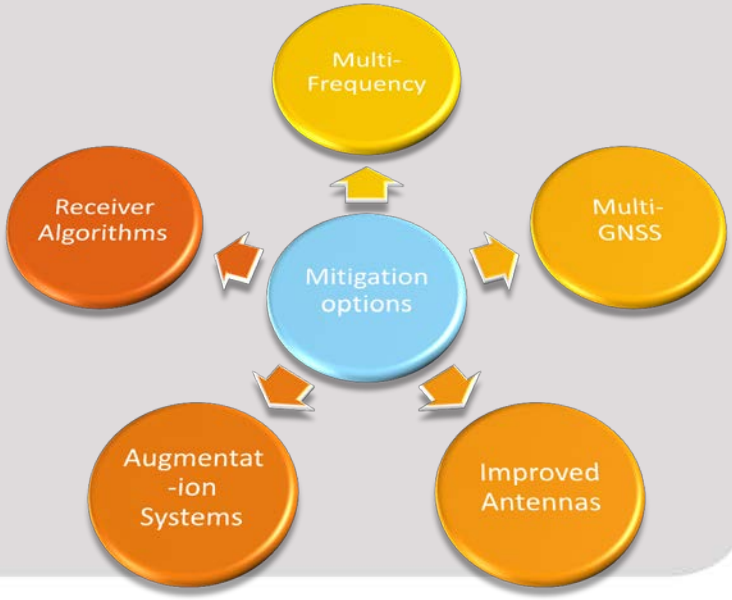
RPNT framework

Risk Assessment → Test vs threats → Implement mitigation strategy

Detection and characterisation of environment

Use the RPNT framework to highlight the most appropriate and cost effective improvement areas…..

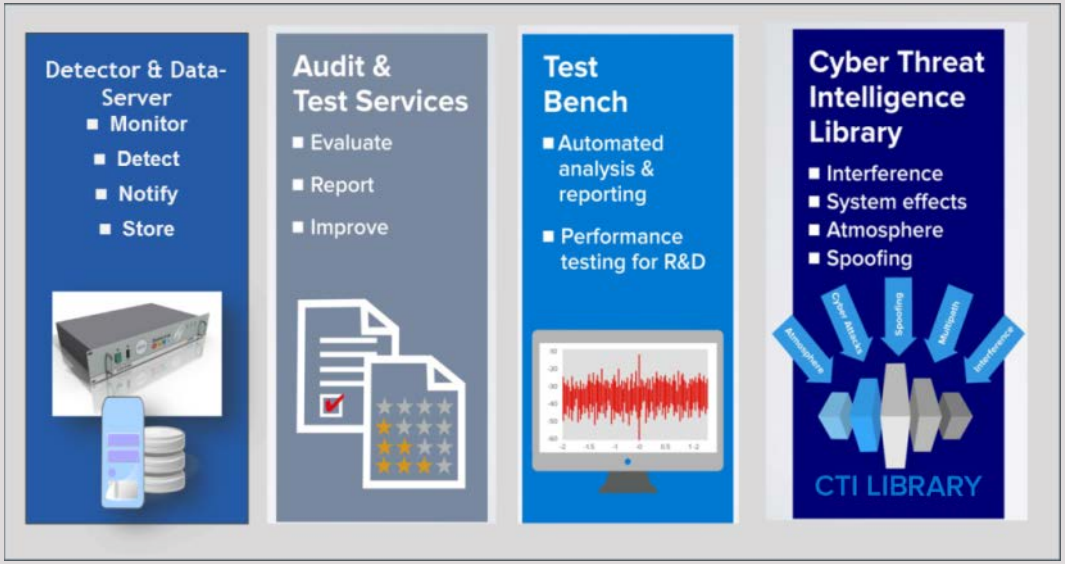




- GPS / GNSS has unique advantages and will remain as a key component for Position, Navigation and Timing for the foreseeable future
- Interference threats are widespread – the GNSS spectrum isn't clean
- Our evidence shows that GNSS interference can affect PNT systems in unexpected ways
- Important not to be left in the dark – Don't leave it to guesswork
  - Carry out Risk Assessment including testing against the latest real-world threat baseline
  - Aim for an informed mitigation strategy based on quantitative data

Image source Twitter/SimonOstler as published in Hack.com

Thank You



Join the GNSS Vulnerabilities group on LinkedIn to find out more about GNSS jamming and spoofing and join the discussion

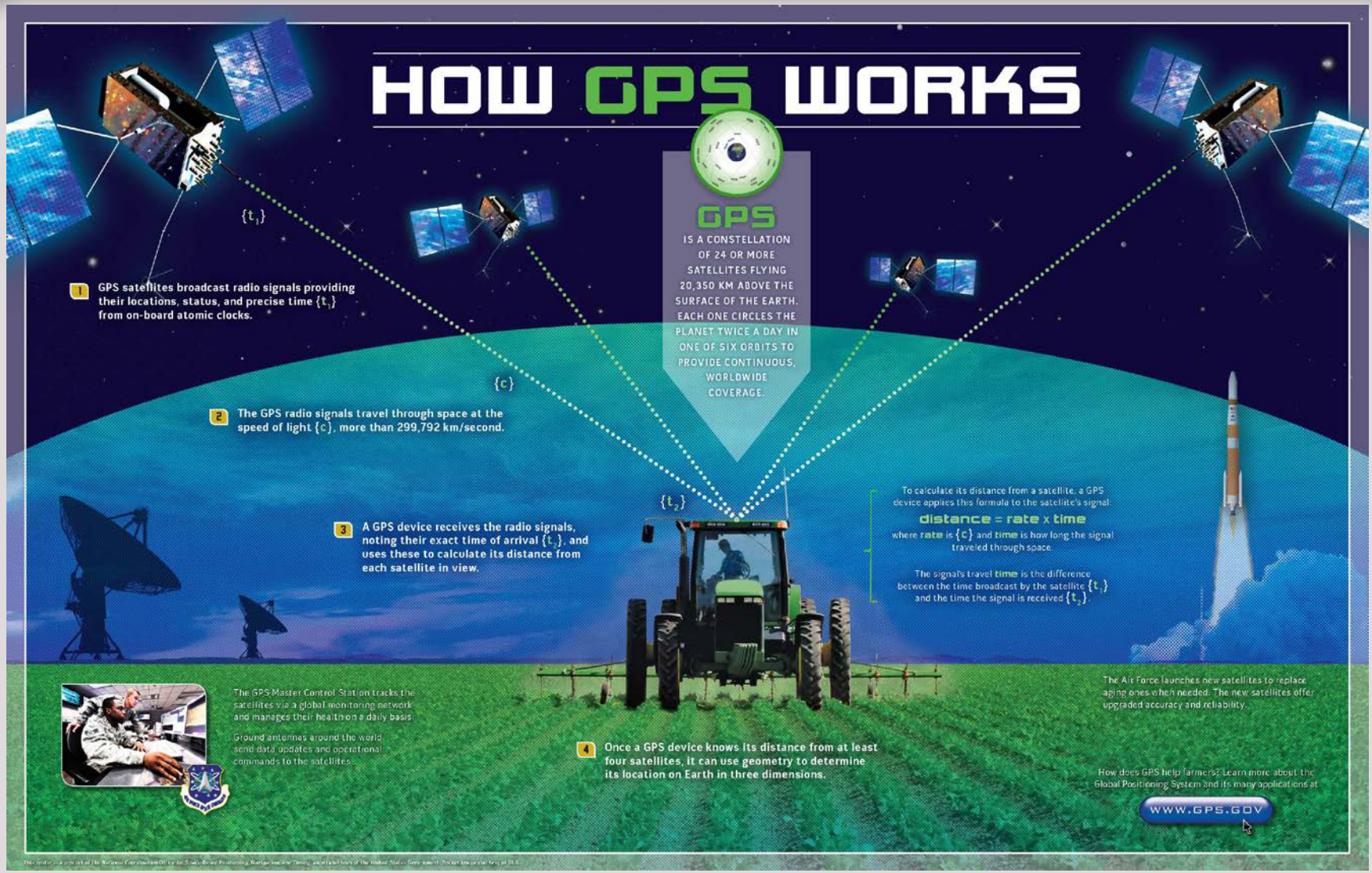
Interference Detection and Mitigation and GNSS Jammers

Rick Hamilton
U.S. Coast Guard
Navigation Center

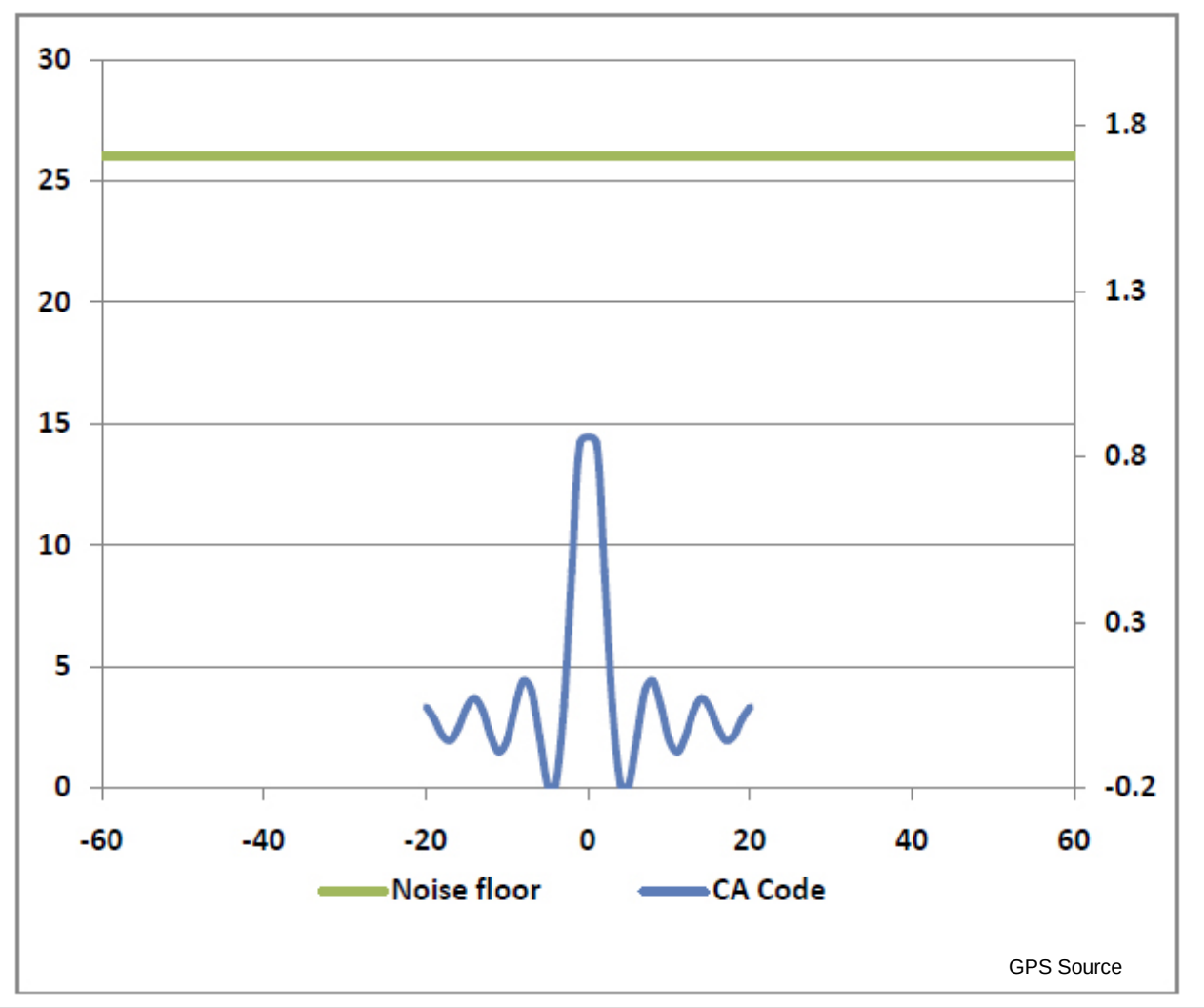
Overview

- Why Protect GNSS Frequencies?
- What are Jammers?
- How do Jammers Work?
- Proliferation of jammers
- Illegal use
- Coordinated government response to interference events
- Regulations to prohibit manufacture, import, export, sale and use of jammers

Very Weak Space-to-Earth Signal (-163 dBW)



GPS Signal is Hidden Beneath the Noise Floor



Governments have strict processes to be authorized to conduct testing on GPS frequencies. Examples:

- Federal Agencies for receiver resilience testing
- Department of Defense for military receivers
- Commercial companies
- Receiver manufacturers

All these license applications go through FCC and/or NTIA for authorization to generate interference on a GPS frequency for testing purposes.

NAVCEN routinely receives interference reports from all over the world:

- International Airlines have reported complete loss of GPS on air routes over Iran
- In 2010 interference began in Korea with reports to NAVCEN from 9 separate commercial airlines

[The Central Radio Management Office, South Korea]

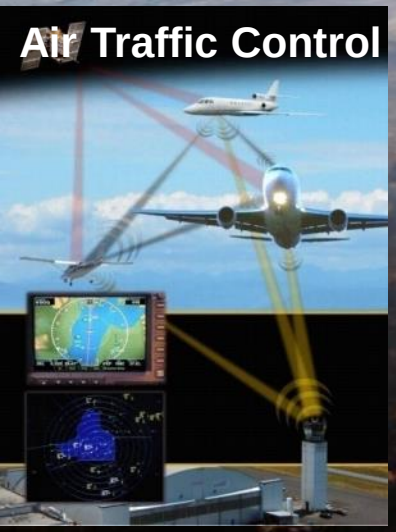
Dates	Aug 23-26, 2010 **(4 days)**	Mar 4-14, 2011 **(11 days)**	Apr 28 – May 13, 2012 **(16 days)**
Jammer locations	Gaesong	Gaesong, Mt. Gumgang	Gaesong
Affected areas	Gimpo, Paju, etc.	Gimpo, Paju, Gangwon, etc.	Gimpo, Paju, etc.
GPS disruptions	**181 cell towers, 15 airplanes, 1 battle ship**	**145 cell towers, 106 airplanes, 10 ships**	**1,016 airplanes, 254 ships**

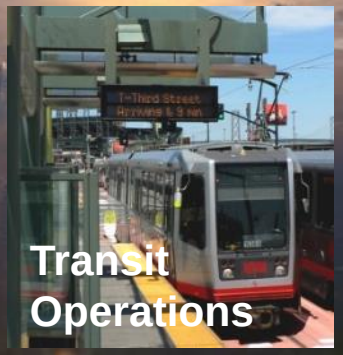
Generally includes devices commonly called signal blockers, GPS jammers, cell phone jammers, text blockers, etc

- Illegal radio frequency transmitters
- Designed to block, jam, or otherwise interfere with authorized radio communications

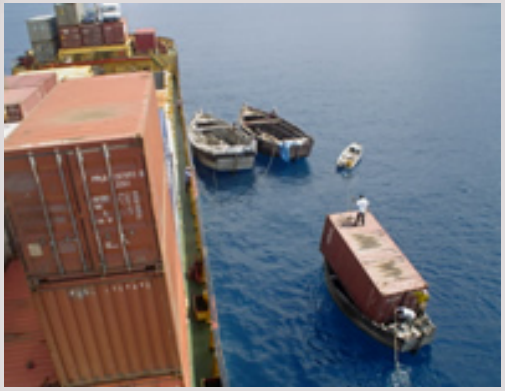
Jammers are Prohibited:

They can have broad impacts on individual users and critical infrastructure





- A jammer can *block all radio communications* on any device that operates on radio frequencies within its range.
- *Emits radio frequency waves* that prevent the targeted device from establishing or maintaining a connection.
- Generally *does not discriminate* between desirable and undesirable communications.
- Jammers can:
  - prevent your cell phone from making or receiving calls, text messages, and emails;
  - prevent your Wi-Fi enabled device from connecting to the Internet;
  - prevent your GPS unit from receiving correct positioning signals; and
  - prevent a first responder from locating you in an emergency.



One ship can bring as many as 19,000 20ft containers

http://www.marinevesseltraffic.com

Shanghai Harbor: 33.62 million TEUs in 2013.

Known incidents of Interference

- Jammers overwhelm anti-theft devices on cars and trucks. 46 luxury cars returned to Port of Los Angeles discovered with GPS jammers attached to the batteries
- Have been used in vicinity of airports disrupting air traffic

- Establishing quiet zones and text-free zones in Churches and Schools

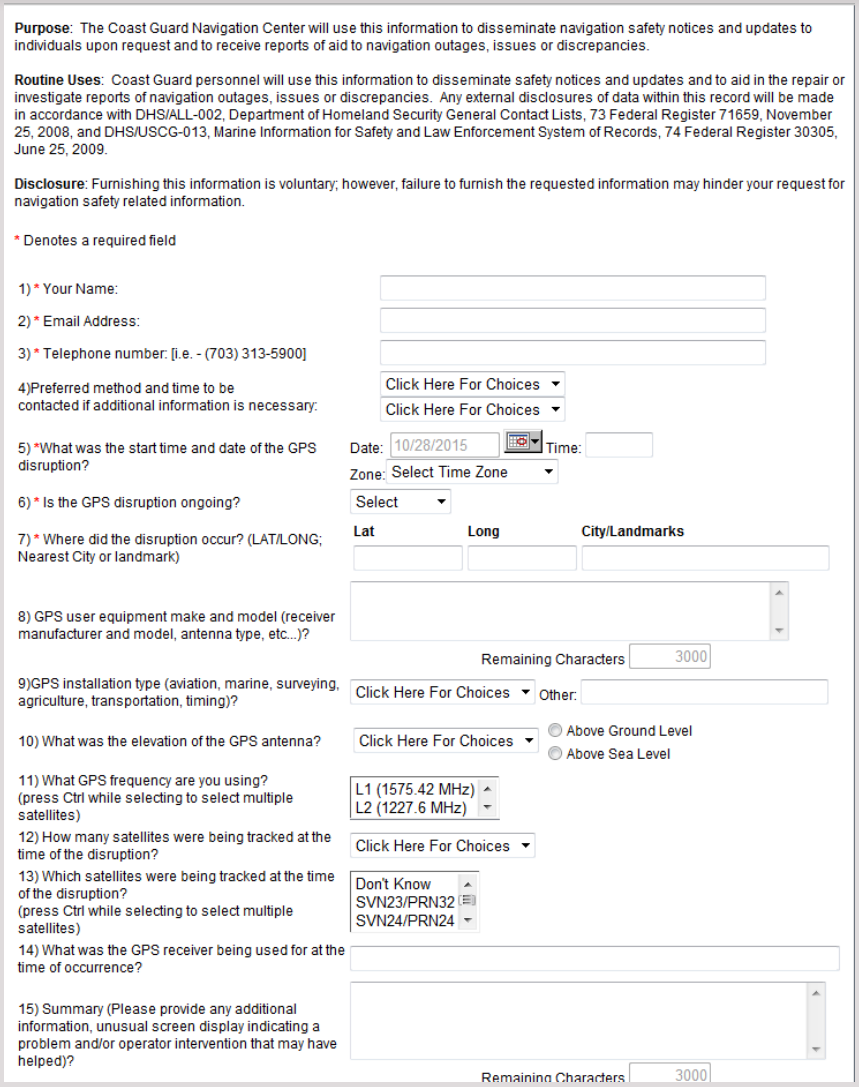
- Used to disrupt communications during commission of a robbery
- Used in vicinity of a major port disabling GPS on large cruise ships attempting to dock

- Used to defeat the fleet tracking devices in company cars and trucks for theft of high value pharmaceuticals
- Used to defeat attempts to document road use for taxes
- **These uses of jammers are <u>all illegal</u>**

Interference Reporting

U.S. process starts with problem report to NAVCEN or FAA

- Different than ITU form
  - Problem Rpt vs After Action Rpt
- Service Center triage to confirm problem
- Initial interagency conference call to provide for a coordinated government response/Discussion on way fwd
- Priority assigned will determine level of response and agencies involved



Purpose: The Coast Guard Navigation Center will use this information to disseminate navigation safety notices and updates to individuals upon request and to receive reports of aid to navigation outages, issues or discrepancies.

Routine Uses: Coast Guard personnel will use this information to disseminate safety notices and updates and to aid in the repair or investigate reports of navigation outages, issues or discrepancies. Any external disclosures of data within this record will be made in accordance with DHS/ALL-002, Department of Homeland Security General Contact Lists, 73 Federal Register 71659, November 25, 2008, and DHS/USCG-013, Marine Information for Safety and Law Enforcement System of Records, 74 Federal Register 30305, June 25, 2009.

Disclosure: Furnishing this information is voluntary; however, failure to furnish the requested information may hinder your request for navigation safety related information.

* Denotes a required field

1) * Your Name:

2) * Email Address:

3) * Telephone number: [i.e. - (703) 313-5900]

4)Preferred method and time to be contacted if additional information is necessary: Click Here For Choices / Click Here For Choices

5) *What was the start time and date of the GPS disruption? Date: 10/28/2015 Time: Zone: Select Time Zone

6) * Is the GPS disruption ongoing? Select

7) * Where did the disruption occur? (LAT/LONG; Nearest City or landmark) Lat Long City/Landmarks

8) GPS user equipment make and model (receiver manufacturer and model, antenna type, etc...)? Remaining Characters 3000

9)GPS installation type (aviation, marine, surveying, agriculture, transportation, timing)? Click Here For Choices Other:

10) What was the elevation of the GPS antenna? Click Here For Choices Above Ground Level Above Sea Level

11) What GPS frequency are you using? (press Ctrl while selecting to select multiple satellites) L1 (1575.42 MHz) L2 (1227.6 MHz)

12) How many satellites were being tracked at the time of the disruption? Click Here For Choices

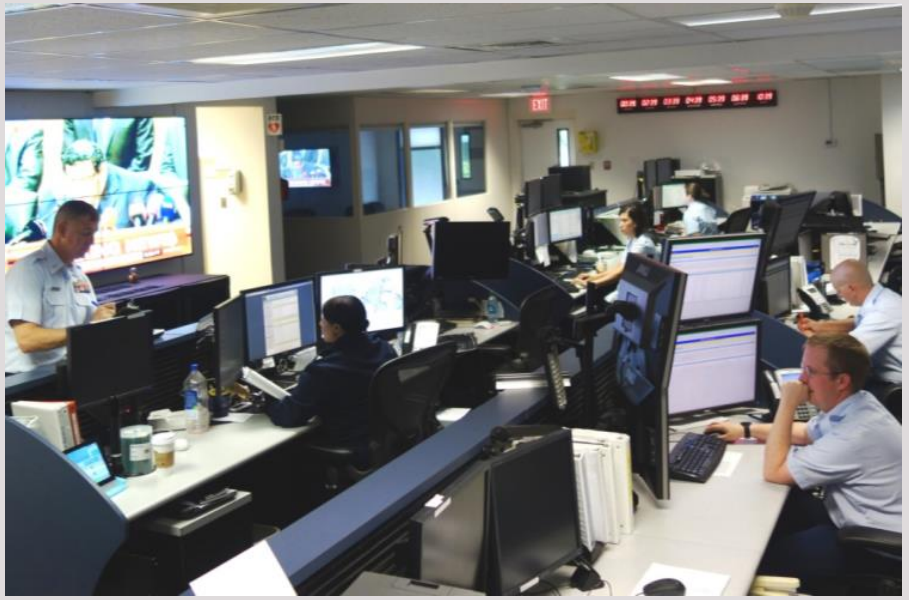
13) Which satellites were being tracked at the time of the disruption? (press Ctrl while selecting to select multiple satellites) Don't Know SVN23/PRN32 SVN24/PRN24

14) What was the GPS receiver being used for at the time of occurrence?

15) Summary (Please provide any additional information, unusual screen display indicating a problem and/or operator intervention that may have helped)? Remaining Characters 3000

Initial Operating Capabilities (IOC) 2015

- Currently testing functionality and capabilities
- Collaboration tool.
- Text based Log displays.
- Allows for attachments.
- Archives all events for documentation and later analysis.



•Full Operating Capabilities (FOC) plan to include the following features:

- Collaboration tool. Automatic e-mail distribution when new Events are reported
- Text based Log displays. Ability to view data geographically in a Web-Based Map viewer

Ask the Experts – Part 1

Guy Buesnel
CPhys,FRIN
Spirent

Rick Hamilton
U.S. Coast Guard Navigation Center

Grace Gao
Asst. Professor Aerospace Engineering University of Illinois Urbana-Champaign

Poll #2

While they are illegal to use, purchasing a personal privacy device is legal in:

a. United States
b. People's Republic of China
c. European Union
d. Russian Federation
e. Not legal in any of the above.

Part II

Rick Hamilton
U.S. Coast Guard
Navigation Center

U.S. Federal statutes and regulations generally prohibit the manufacture, importation, sale, advertisement, or shipment of devices, such as jammers.

In order to be completely effective, in the U.S. laws are generally instituted in four different authorities:

- U.S. Federal Statutes – Legislation
- Telecom Agency Rules – FCC
- The Criminal Code
- International Treaties

U.S. Federal Statutes – Communications Act

- 47 U.S.C. § 301 Unlicensed (unauthorized) operation prohibited.
- 47 U.S.C. § 302a(b) Manufacturing, importing, selling, offer for sale, shipment or use of devices which do not comply with regulations are prohibited
- 47 U.S.C. § 333 – Interference to authorized communications prohibited
- 47 U.S.C. § 503: Forfeitures (monetary fines)
- 47 U.S.C. § 510: Forfeiture of communications devices

Regulations in the U.S.
Telecom Agency Rules – FCC

- 47 C.F.R. § 2.803(a) marketing is prohibited unless devices are authorized and comply with requirements

- 47 C.F.R. § 2.803(e)(4) – marketing is defined as "sale or lease, or offering for sale or lease, including advertising for sale or lease, or importation, shipment, or distribution for the purpose of selling or leasing or offering for sale or lease."

Title 18 of the U.S. Code (U.S.C.) contains the criminal and penal code of the U.S. government. It addresses federal crimes, criminal procedures, and general provisions. Prohibits on acts that:

- Destroy or endanger an aircraft or endangering the safety of any such aircraft in flight.
- Interference with a navigation facility
- Communication of information known to be false
- Interference to U.S. government communications;
- malicious interference to satellite communications

Violation subjects operator to possible fines, imprisonment, or both

- 49 U.S.C. section 46308 and 18 U.S.C. sections 32(a)–35 are referenced within FAA Order 6050.22c [5-3], which contains procedures for investigating and reporting radio frequency interference affecting the U.S. National Airspace (NAS).

- FAA Order 6050.22c includes an interagency agreement between the FAA, Federal Bureau of Investigation, and FCC on procedures the three agencies should follow to effectively interact in an attempt to locate, identify, and resolve any deliberate RFI acts such as “phantom controller” incidents.

- The United Nations Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation is a multilateral treaty that was adopted by the International Conference on Air Law at Montreal on 23 September 1971.

- The Convention signatories agree to prohibit and punish acts that threaten the safety of civil aviation. It entered into force on 26 January 1973 after ratification by 10 nations. As of today, the Convention has 188 signatories.

- Several of the U.S. laws relevant to intentional interference and spoofing of civil aviation GNSS applications mentioned above were enacted to satisfy obligations made per this Convention.

GNSS Jammers – National Legal Status

Jammers	US	RU	China	EU
manufacture	illegal	illegal	illegal	Nation-by-nation
sell	illegal	illegal	illegal	illegal
export	illegal	illegal	illegal	Nation-by-nation
purchase	Undefined (consumer import illegal)	illegal	illegal	illegal
own	legal	Undefined	Undefined	legal
use	illegal	illegal	illegal	illegal

The ICG recommends that GNSS providers and GNSS user community member states evaluate existing and emerging interference detection, localization, and characterization capabilities and consider developing, testing and implementing these or similar capabilities in their nations or regions of the world

ICG Interference Detection and Mitigation Workshops

- Workshop participants encourage system providers and user community members to evaluate the interference detection and characterization capabilities of the EU-funded DETECTOR project and consider testing a similar capability in other regions.

- Chronos Technology presented a briefing on the UK Sentinel Project targeting small jammers being used to defeat road use/tax monitoring. http://www.chronos.co.uk/files/pdfs/gps/SENTINEL_Project_Report.pdf

- Design Bureau «Vektor», Russia presented general guidelines and practical example of the analysis of spatial distribution of emissions in the frequency bands of GNSS

- Harris Corporation presented information about their Signal Sentry 1000 system, demonstrating a real-time geo-location system

https://www.youtube.com/watch?feature=player_detailpage&v=bAK8Yil-njA

System providers and user community member states are encouraged to work with industry groups to determine if standards for crowd sourcing interference detection and localization techniques should be developed and cost-effectively implemented by mobile telecom service providers.

Discussed at June 2015 IDM Workshop

- May be better for detection networks to begin with cell towers instead of mobile phones
- Volume of data from nation-wide system may not be practical; regional monitoring centers might be more realistic.
- Consensus that efforts aimed at initiating crowd-sourcing should begin with discussions between Task Force and individual companies before approaching user industry organizations such as 3GPP
- Industry may be reluctant to act without market demand or government intervention through laws or regulations

Way Forward

- WG-A requested Task Force to invite industry representatives to WG-A Meeting at ICG-10 to show how crowd-sourcing would work and discuss the feasibility
- Crowd Sourcing may also be discussed further at the next IDM Workshop

Conclusion

- The threat from jammers is real and growing.
- Jammers are being used to commit crimes
- “Personal Privacy Jammers” are being used to defeat company tracking and worse.
- ICG recommendations and IDM workshops are being conducted to make developing countries aware of the benefits and efficiencies of GNSS use.
- Included in these workshops now are sessions devoted to IDM to promote the establishment of laws to curb the proliferation and illegal use of Jammers around the world.

U.S. Coast Guard Navigation Center Contact Information

http://www.navcen.uscg.gov

E-mail: nisws@navcen.uscg.mil
Phone: +1 703 313 5900
Fax: +1 703 313 5920

Civil GPS Service Interface Committee Secretariat

E-mail: rick.hamilton@uscg.mil

Protecting GNSS Receivers from Jamming and Interference

Grace Gao
Asst. Professor
Aerospace Engineering
University of Illinois
Urbana-Champaign

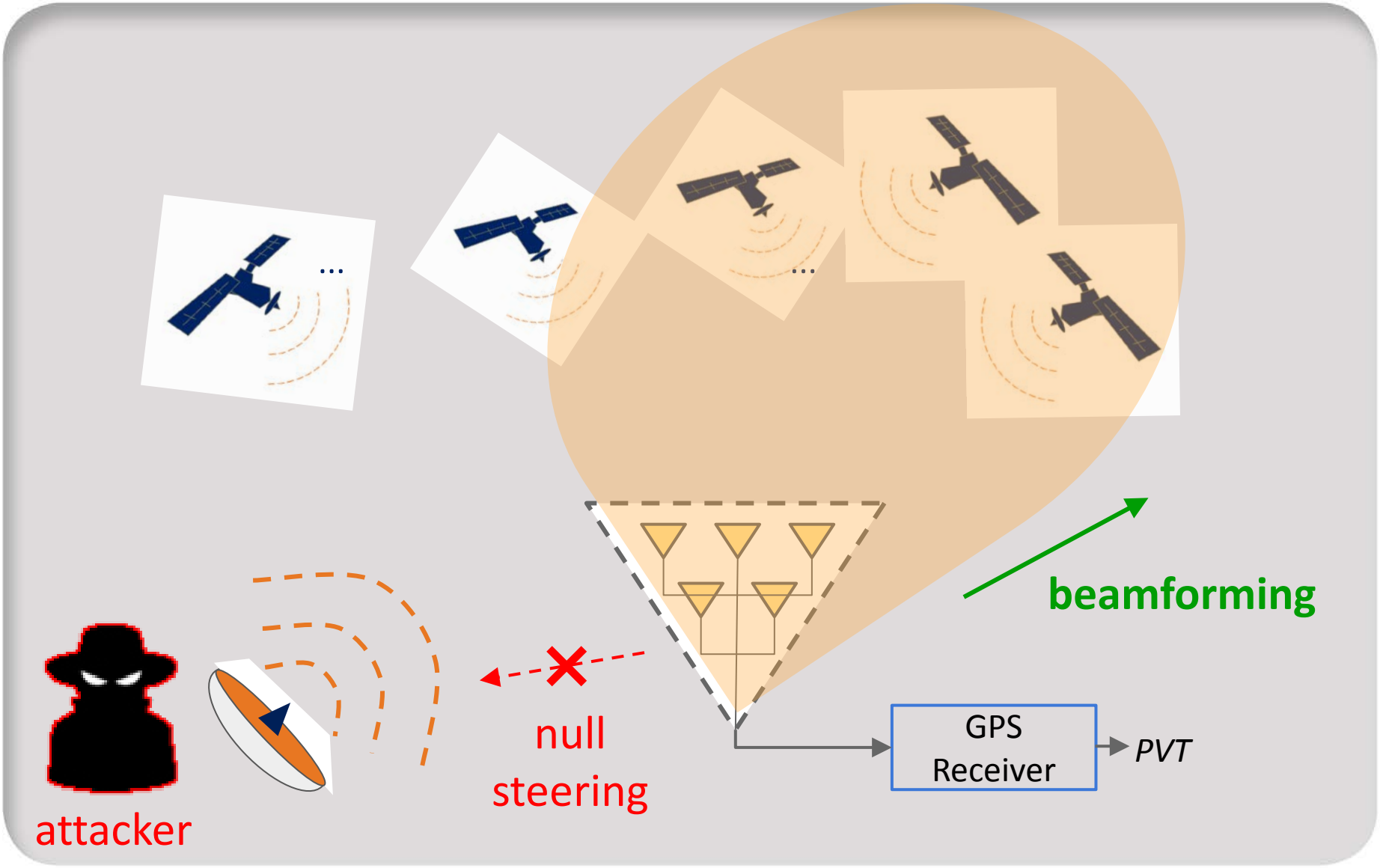
Know your enemy

- Interference is local
- Interference is on/near the ground
- Interference aimed at GPS frequencies

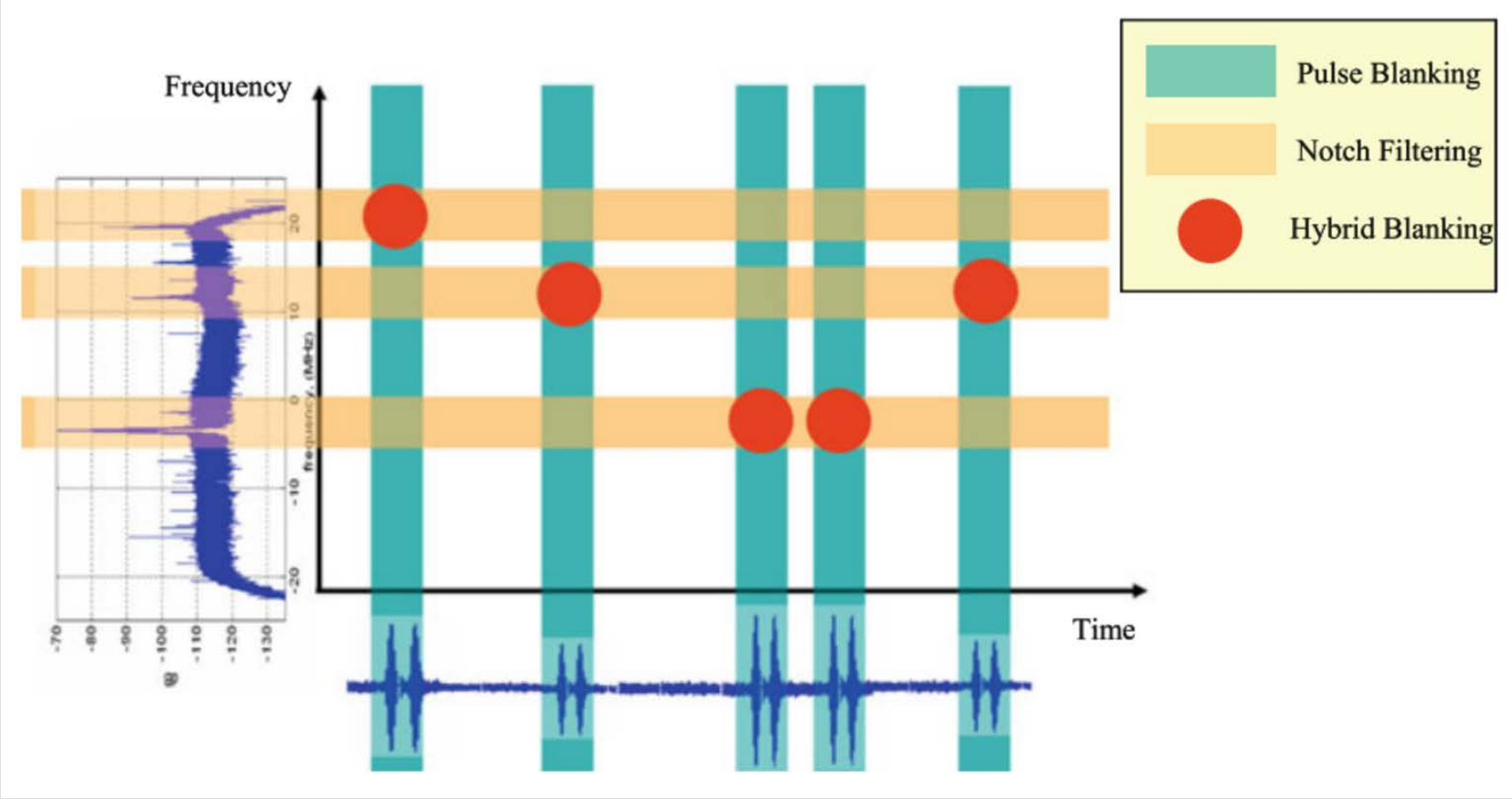
Know yourself

- GPS is global
- GPS satellites are >20,000km above
- Navigation sensors other than GPS
- Hardening GPS processing

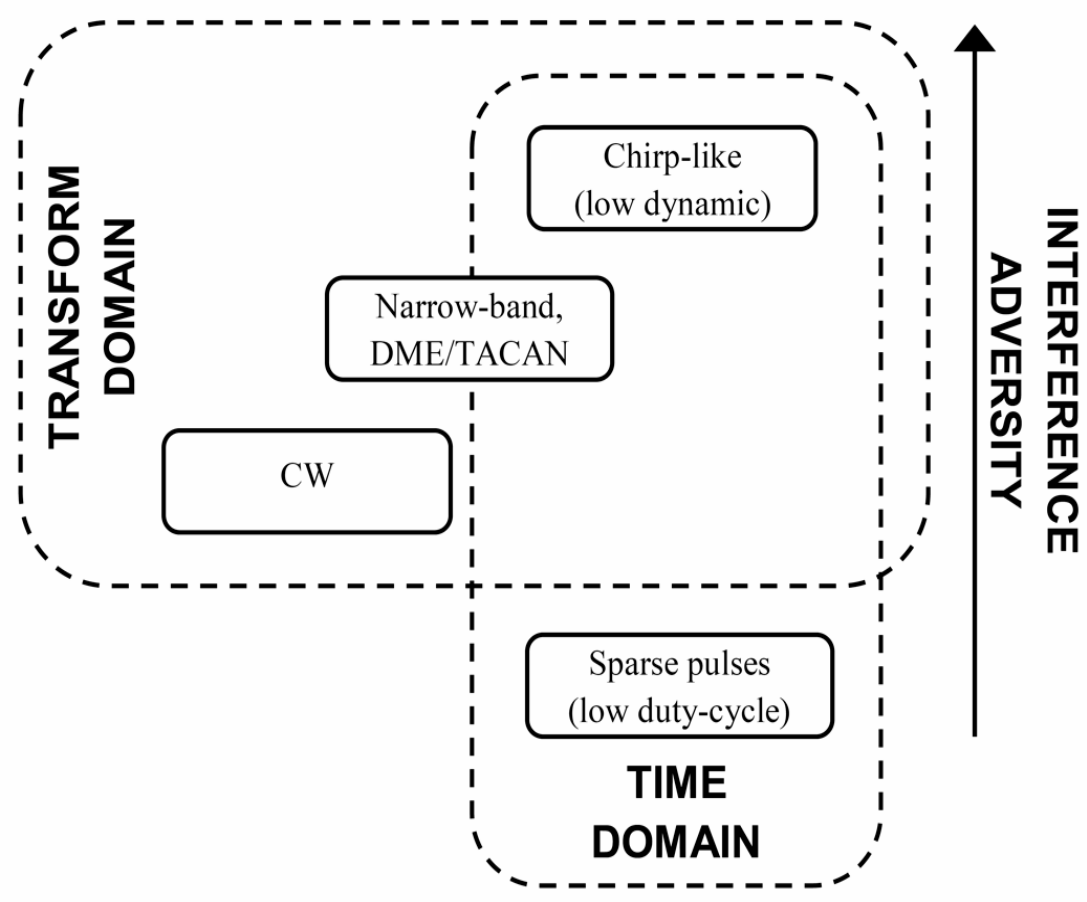
- Spatial filtering
- Time-frequency filtering
- Inertial aiding
- Vector tracking
- Direct positioning


beamforming
null
steering
attacker
GPS
Receiver
PVT

Example: DME interference mitigation

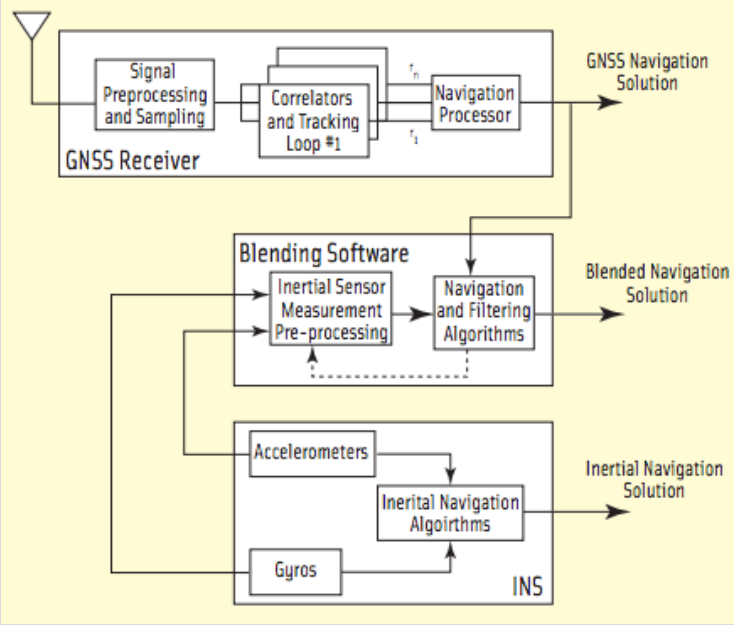


G.Gao, et al., GPS Solutions 2013

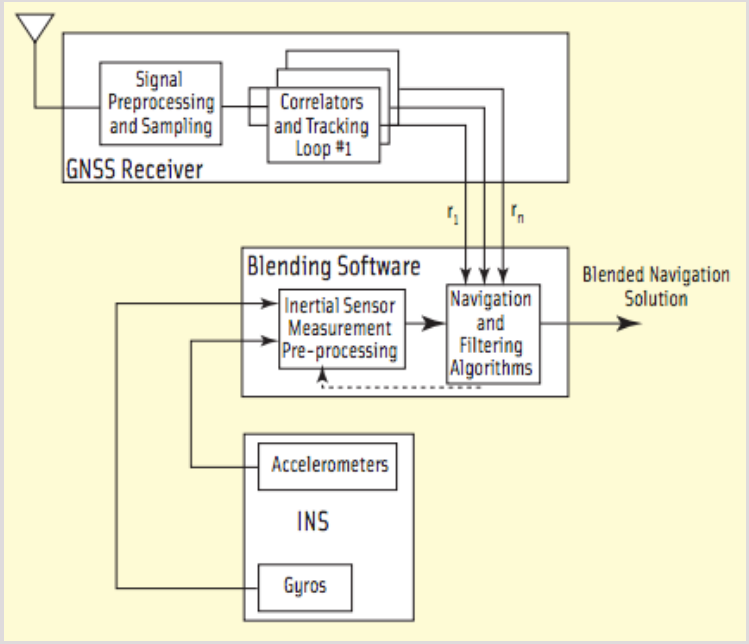


G.Gao, et al., Proceedings of IEEE, 2016 (to appear)

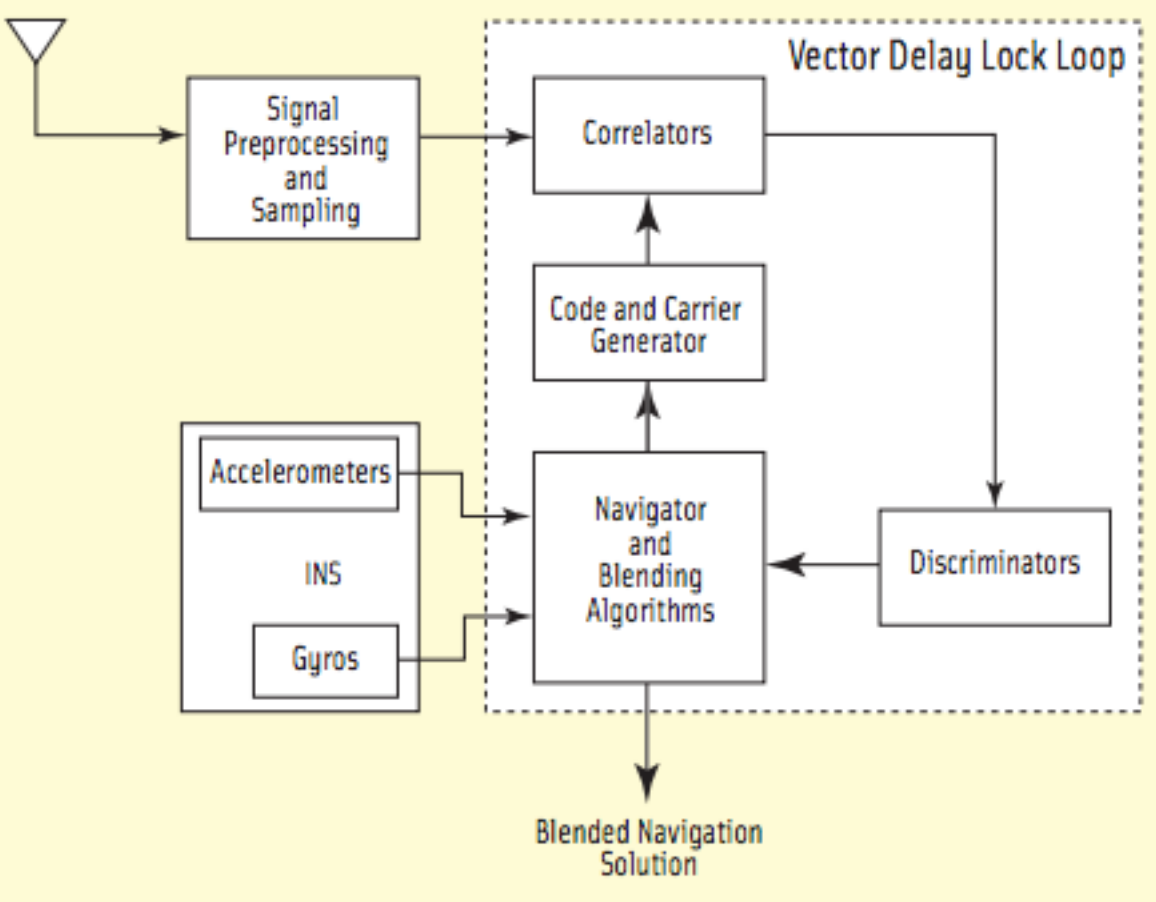
Loosely coupled:
GNSS positions + INS



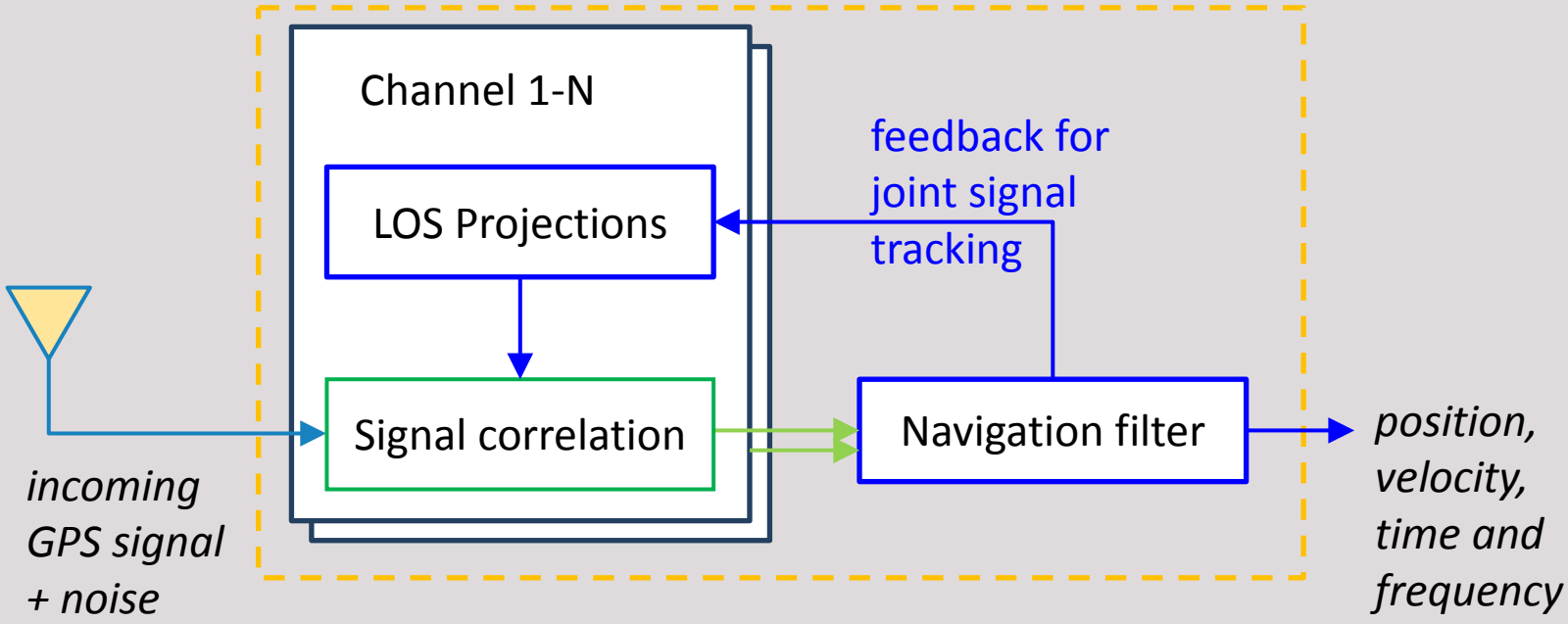
Tightly coupled:
GNSS measurements + INS

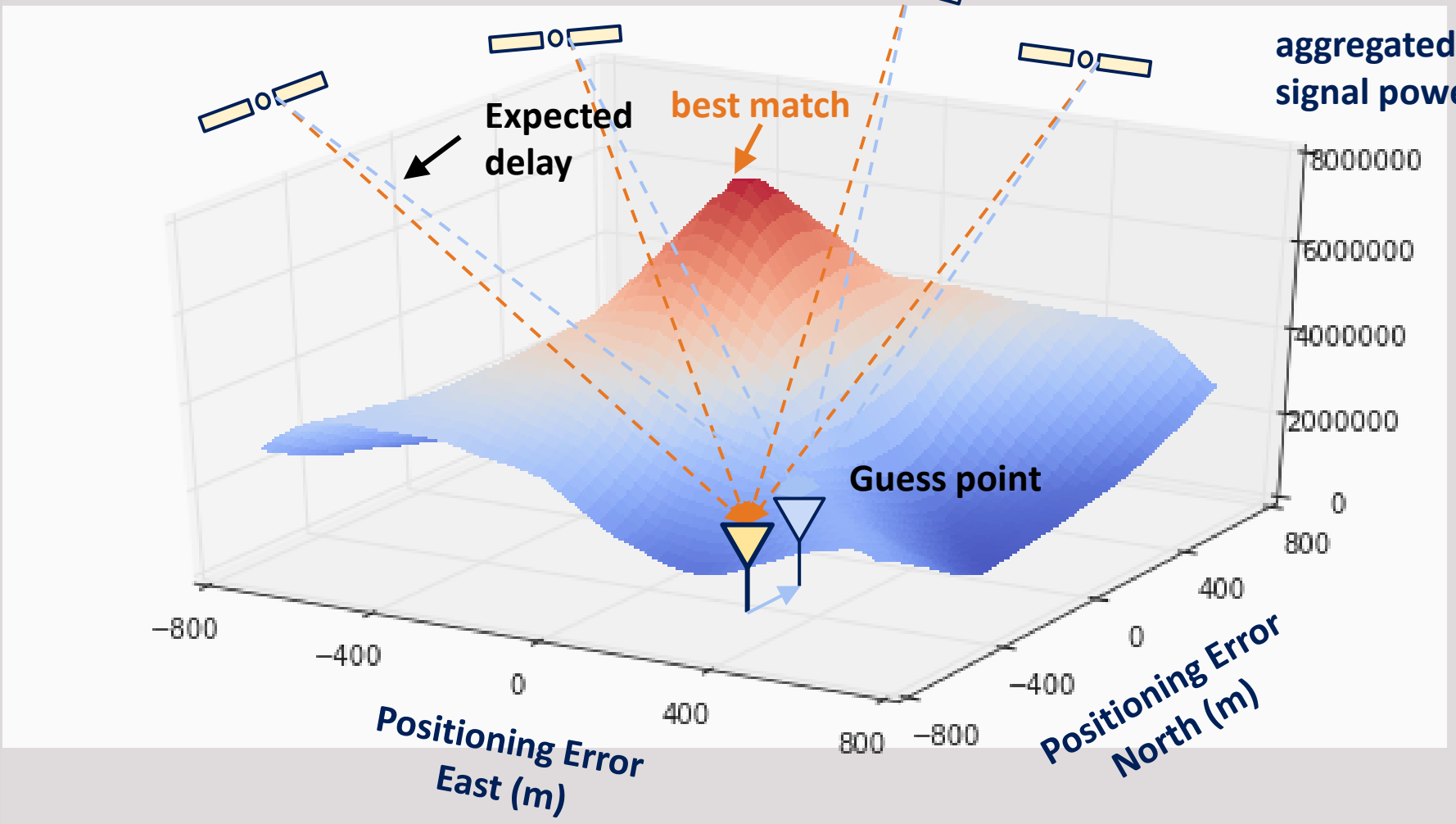


Gebre-Egziabher, InsideGNSS 2007



Gebre-Egziabher, InsideGNSS 2007


Channel 1-N
LOS Projections
feedback for joint signal tracking
Signal correlation
Navigation filter
incoming GPS signal + noise
position, velocity, time and frequency



Y.Ng and G.Gao, ION PLANS 2016

- Spatial filtering
- Time-frequency filtering
- Inertial aiding
- Vector tracking
- Direct positioning

Next Steps

- **Visit www.insidegnss.com/webinars** for a PDF of the presentations and a list of resources.
- Review the recorded version of today's webinar

Contact Info:

- **Inside GNSS- www.insidegnss.com**
- **Novatel - www.novatel.com/**

Poll #3

Which of the following best describes your experience?

a. I have experienced signal interference in the last few years.
b. I've never experienced signal interference.
c. I'm not sure if I have ever experienced signal interference.

Ask the Experts – Part 2

Guy Buesnel
CPhys,FRIN
Spirent

Rick Hamilton
U.S. Coast Guard Navigation Center

Grace Gao
Asst. Professor Aerospace Engineering University of Illinois Urbana-Champaign

Inside GNSS @ www.insidegnss.com/
www.novatel.com/