Threats to GPS and the US Response

Presented by Les Berry / David Jones

13 May 2019

GENERAL DYNAMICS
Mission Systems

GPSS

Overview / Abstract

The US Department of Defense is moving forward with upgrading and improving Positioning, Navigation, and Timing (PNT) equipment. Three major programs, Modernized GPS (M-Code), an Assured PNT Program of Record, and an effort led by the US Army Rapid Capability Office, will allow US forces unhindered access to trusted PNT in all environments. GPS Source, an industry leader in Assured PNT, is the prime contractor for the US Army's M-Code integration effort. In addition, our equipment has been selected as a candidate for the program of record and is being fielded as part of an Operational Needs Statement (ONS). GPS Source has a unique perspective to the challenges of implementing Assured PNT in challenging military environments.

The purpose of this talk is to update the international community on the status of those efforts and discuss methods to establish a capability for providing uninterrupted and valid PNT.

Operational Realities

- An uninterruptable and reliable source of Positioning, Navigation & Timing (PNT) data is required for virtually all Platform C4ISR/EW client systems.
- Most US Army ground vehicles are required to use GPS as their primary source of PNT.
- GPS is a weak, space-based signal and is vulnerable to denial or spoofing attacks.
- Exploitation of GPS vulnerability is rapidly becoming a strategy of near peer and unsophisticated adversaries. Jamming (disruption of GPS signals) and spoofing (broadcast of incorrect GPS signals) are becoming standard Electronic Warfare tactics in virtually every operational theater.
- Denial of GPS reduces the ability of the warfighter to shoot, move, and communicate and results in significant degradation of combat power.

Impact of Loss of Accurate PNT

- **Ground Vehicles** will lose positional data
  - Results in decreased ability to accurately navigate.
- **Command and Control** systems will lose positional awareness
  - Results in decreased ability to coordinate battlefield activities.
- **Fire Control Systems** will suffer diminished precision from loss of GPS-aided solution
  - Results in less accurate fire support
- **Counter-IED** and **Communication** systems will lose time accuracy
  - Results in degraded communications and IED protection.

Recent Reports of GPS Denial/Deception

2011 – Iran / US RQ-170 Drone Incident

- Iran captured and landed a drone using cyber attack equipment

2014 – Ukraine forces experience GPS muting during attacks

2017 – Ships in Black Sea reported GPS position errors locating them at Sochi Airport (~40km away)

- At least 20 vessels reported erroneous GPS readings
- All research has attributed this to a deliberate “spoofing” attack

2019 – Finland reports widespread GPS denial attack during joint NATO training exercise

2019 – The Center for Advance Defense Studies publishes a paper detailing 9,883 spoofing attacks from February 2016 to November 2018.[1]

US Government Actions

The US Government has taken significant steps to address the threats to US warfighters:

- A new Assured PNT Cross Functional Team established. The APNT CFT has been tasked to reduce the time to deliver new weapons systems, which includes a significant reduction of the requirements development process to 12 months or less.[2]

- The GPS satellite constellation is being modernized and is broadcasting a new GPS signal (M-Code). New GPS receivers will be needed to utilize the M-Code signal. The Military GPS User Equipment (MGUE) effort includes developing Lead Platforms for each branch of the US Department of Defense (Army, Navy, Air Force, Marines).[3]

US Government Actions

The US Government has taken significant steps to address the threats to US warfighters:

- The Rapid Capabilities and Critical Technologies Office (RCCTO) has worked in conjunction with Project Manager Positioning Navigation and Timing (PM PNT) to develop a point protection system that will allow soldiers to continue to maneuver in a GPS challenged environment.[4]

- Project Manager Positioning Navigation and Timing has initiated a formal Program of Record to develop a Mounted PNT device that will provide Assured PNT to client platforms and systems.[5]

M-Code User Equipment

- The US Army Lead Platform for M-Code is the **Enhanced DAGR Distributed Device (ED3)** installed on a Stryker vehicle.[6] The international version of the ED3 is called the "**Enhanced FLO-G**"

- Operational User Assessment scheduled to be completed in 2021.[7]

- Non-US Availability: "The current policy allows for the sale of M-code equipment to all 57 authorized GPS PPS nations. The M-code technology will be made available to these nations through the Foreign Military Sales process." – US Air Force GPS Directorate [8]

Enhanced DAGR Distributed Device (ED3) – U.S. Enhanced FLO-G - Non U.S.

Replaces up to four DAGR units in a single vehicle

- Performs all DAGR functions (RS232, RS422, SINCGARS Mode3 TOD)
- Reduces cost & space requirements compared to multiple DAGR's.

Uses a single GPS receiver card to distribute PNT Data

- Can host either a SAASM GB-GRAM or an M-Code receiver card (upgradable).
- Can host either a Type 1 or Type 2 (smaller) form factor GPS receiver card.

Can distribute messages to various client systems

- IS-GPS-153, NMEA0183, or MSID (M-Code) formats
- Each output port can be independently configured to comply with unique client system requirements:
  - Lat/Long format vs MGRS.
  - Various baud rates and datums.

Enhanced D3 (U.S.)
(Enhanced FLO-G – Outside U.S.)

U.S. Army RCCTO: "Program T"

- "Program T" is a unit specific effort intended to provide certain units in Europe with area and point protection systems that detect threats to GPS and will allow vehicles to maneuver in a GPS denied environment.[9]

- The mounted system will provide platform PNT assurance (continual access to PNT with a high level of integrity). [10]

- The mounted system, based on the **ED3**, will be fielded in Europe starting in 2019.[11]

Current Assured PNT Solution

A Basic Assured PNT System consists of:

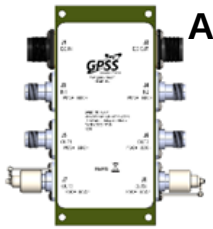
- Enhanced D3 (ED3) / E-FLO-G
  - PNT distribution
- VICTORY/CSAC Accy. Module (VCAM)
  - Hosts ES/EP and generation of precise timing
- Electronic Surveillance/ Electronic Protection Software (ES/EP)
  - Detects threats to GPS
- Anti-Jam Antenna System (AJAS)
  - Mitigation of enemy jammer capabilities
- Anti Jam Antenna Integration Module (AJAIM)
  - Allows low power standby mode for Anti Jam Antenna and allows for redundant GPS antenna capability
- Fixed Reception Pattern Array (FRPA) Antenna
  - Receives broader electromagnetic spectrum to support ES/EP capabilities

Enhanced D3 / Enhanced FLO-G

VCAM

ES/EP SW

AJAS



AJAIM

FRPA

Assured PNT P.O.R: "Program M"

- Intent is to develop a scalable, upgradeable system-mounted platform for ground and unmanned aerial vehicles by fusing GPS with alternate navigation and timing technology to provide trusted PNT to client platforms and systems. It will distribute PNT data to multiple systems directly and via the network, replacing the need for multiple GPS devices on a single platform. [12]
- Three vendors have been chosen and their prototype systems are currently being evaluated. It is anticipated that at some point during the Program of Record the Government will offer an upwards invitation to a single vendor.
- The Program will take part in three phases:
  - Phase 1 – Initial Evaluation (6 months)
  - Phase 2 – Test Fix test (15 months)
  - Phase 3 – Operational User Assessment (15 months)
- Fielding quantities are unknown at this time
- ED3/VCAM and Anti-Jam Antenna have been designated as "Program M" Gen. 1 [13]

Summary

- US DoD is energetically addressing threats to GPS.
  - New organizational structure
  - Urgent responses to Theaters
  - Program of Record
  - Updating the entire GPS (Ground stations, satellites, and user equipment)
- M-Code will not be available to non-US customers for several years.
- The Program of Record solution will not be fielded for several years.
- A US Army qualified and approved Assured PNT solution is being fielded in Theater and is available today.

Questions, Comments, Contact Info

For more information on Assured PNT, Assured PNT Products, and GPS/PNT Threat Mitigation contact:

Les Berry
International Business Development
Lester.Berry@gd-ms.com

David Jones
Solutions Architect
David.W.Jones@gd-ms.com

References

Iran / US RQ-170 Drone Incident

- https://en.wikipedia.org/wiki/Iran%E2%80%93U.S._RQ-170_incident

Ukraine forces experience GPS muting

- https://www.realcleardefense.com/articles/2017/05/26/russian_electronic_warfare_in_ukraine_111460.html

Ships in Black Sea reported GPS position errors

- https://www.gpsworld.com/spoofing-in-the-black-sea-what-really-happened/
- https://www.usatoday.com/story/tech/news/2017/09/26/gps-spoofing-makes-ships-russian-waters-think-theyre-land/703476001/

Finland reports widespread GPS denial attack

- https://www.defensenews.com/global/europe/2019/03/08/norway-alleges-signals-jamming-of-its-military-systems-by-russia/

MGUE Benefits and Availability

- https://www.gps.gov/multimedia/presentations/2015/04/partnership/mills.pdf

1 “Russia Is Tricking GPS To Protect Putin”

https://foreignpolicy.com/2019/04/03/russia-is-tricking-gps-to-protect-putin//

2 “Challenge Accepted: APNT CFT Meets Demand for Increased Speed of Delivery”

https://www.army.mil/article/213594/challenge_accepted_apnt_cft_meets_demand_for_increased_speed_of_delivery

3 “GPS / PNT Modernization Progress: State of GPS III, MGUE, Accelerating M-Code, and Resilient PNT”

https://www.gps.gov/governance/advisory/meetings/2018-05/menschner.pdf

4 “Army's PNT programs transition to PEO IEW&S”

https://www.army.mil/article/197066/armys_pnt_programs_transition_to_peo_iews

References

5 “Mounted Positioning, Navigation and Timing”

https://www.pmpnt.army.mil/products/mounted-pnt/

6 “Assured PNT: A Path to Resilient Positioning, Navigation and Timing”

https://www.pmpnt.army.mil/assured-pnt/

7 “New military code about to board 700+ platforms”

https://www.gpsworld.com/new-military-code-about-to-board-700-platforms/

8 “New military code about to board 700+ platforms”

https://www.gpsworld.com/new-military-code-about-to-board-700-platforms/

9 “Army Still Working Long-Term Acquisition Strategy for PNT”

https://www.pmpnt.army.mil/army-still-working-long-term-acquisition-strategy-pnt/

10 “Army Still Working Long-Term Acquisition Strategy for PNT”

https://www.pmpnt.army.mil/army-still-working-long-term-acquisition-strategy-pnt/

11 “Army Rapid Capabilities Office looks to solve challenges on Korean Peninsula”

https://www.c4isrnet.com/digital-show-dailies/ausa/2017/10/11/army-rapid-capabilities-office-looks-to-solve-challenges-on-korean-peninsula/

12 “ASSURED POSITIONING, NAVIGATION AND TIMING (A-PNT) MOUNTED/ANTI-JAM ANTENNA SYSTEM (AJAS)”

https://asc.army.mil/web/portfolio-item/a-pnt-mounted-ajas/

13 “Aberdeen Proving Ground Advanced Planning Briefing to Industry”, MG Kirk F. Vollmecke – PEO IEW&S, 30 April 2019