White Paper
Assured PNT Inside Military Ground Vehicles Using D3

GPS SOURCE

GPS LIVE INSIDE

Brian Paul
December 2013

Introduction

Global Positioning System (GPS) technology has become an integral part of Mission Command systems and military ground vehicle architectures. It plays an important role in the successful execution of tactical missions. The term "GPS" conveys positioning, navigation, and timing (PNT) data, data that is essential in virtually every modern weapon system. Precision timing provides joint forces the capability to synchronize operations and communications. PNT also enables precision attack from stand-off distances, reducing collateral damage and allowing friendly forces to avoid threat areas.[1]

This dependence on GPS may create a weakness and could exemplify the need for the US military to protect PNT sources to assure unhindered access. Few can argue the value of Global Positioning System (GPS) technology in military applications; however, over the past few years, aggressive threats have been identified that place great risk on the use of GPS. Something as simple as a L1 GPS jammer can effectively defeat public toll and vehicle tracking systems. On the battlefield, more complex threats are believed to exist that can defeat or negatively affect L1/L2 GPS receivers, potentially rendering them nearly useless. As a result, the concept of "Assured PNT" has become a prominent topic with military GPS stakeholders around the world. The purpose of this white paper is to discuss the immediate solutions available to achieve the US Army's initiative for "Assured PNT" data, with a focus on military ground vehicle applications. This paper is relevant to US and international users of GPS in ground vehicle architectures.

Assured PNT Strategy

The Army is looking at an Assured PNT strategy that will move from the current state to a System of Systems (SoS) approach. In a ground vehicle environment, this means providing a single PNT distribution solution to multiple devices on the platform. The Army believes this Assured PNT Strategy will help them stay within fiscal constraints, and still offer secure, authenticated access to PNT information.

The Assured PNT strategy will allow access to all sources of PNT, *not just GPS*. It would be based upon three objectives:

- Reduce size, weight and power consumption through the systematic elimination of redundant systems;
- Increase protection to ensure PNT is available and trusted through improvements that keep pace with threats and are scalable;
- Develop ability to migrate M-code GPS informed and guided by the Assured PNT System of Systems Architecture (SoSA).[2]

- The Army is defining their Assured PNT strategy with level-based guarantees to PNT data access and integrity. The level based guarantee of access and integrity are known as PNT Assurance Levels. They range from Level 0 to Level 3. Zero would have the least guarantee of access (equivalent to a commercial GPS). Four (sic)

[1] Prepared under direction of the Chairman of the Joint Chiefs of Staff (2013). *Joint Publication Space Operations*. Retrieved from http://www.dtic.mil/mwg-internal/de5fs23hu73ds/progress?id=FvFRW+49OP

[2] Pinkerton, Mark (2013, December 6) *Assured Positioning, Navigation, and Timing for the Tactical Ground Force.* Retrieved from http://www.arcic.army.mil/Articles/rid-Assured-Positioning-Navigation-and-Timing-for-the-Tactical-Ground-Force.aspx

would have the best guarantee of access (most secure).[3]

Today's PNT Technology

Considering the importance of PNT data to the Warfighter, a growth strategy for Assured PNT is a critical path forward to ensure its safe and continued use in military ground vehicle platforms. However, the US and many friendly nations are currently engaged in operations around the world where PNT signal integrity is important. What technology exists today that improves the fidelity and security of PNT?

Affordability and lifecycle costs are major considerations when evaluating Assured PNT strategies. The US Army's decision to move away from mounted DAGR devices onboard their fleet of vehicles towards a centralized solution in the DAGR Distributed Device (D3) was an excellent example of a decision molded by affordability. But it was also influenced by the D3s ability to eliminate redundant systems, meeting a key objective of Assured PNT on the vehicle platform.

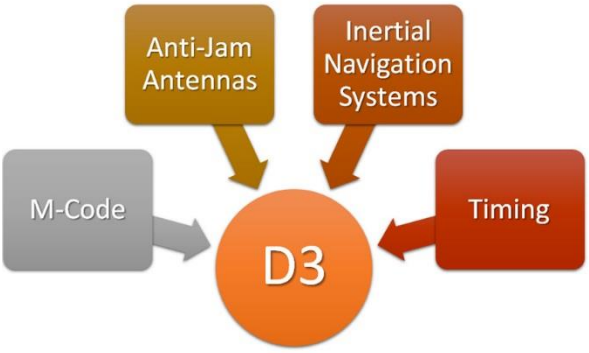
According to the Product Director for PNT in the Program Executive Office for Intelligence, Electronic Warfare, and Sensors:

> *"This is the first device capable of providing platform distribution on mounted platforms with true port independence ... meaning that each system that is plugged into the D3 has full control over the port from the D3, as if the device had its own DAGR."* [4]

This centralized architecture, distributing IS-GPS-153 PNT messages to up to 8 devices inside the vehicle, not only reduces redundancies, but simplifies future migration to M-Code. Eliminating embedded SAASM GPS receivers or peripheral DAGR devices creates a more affordable migration plan to M-code receivers by simply reducing volume and complexity. Further, it provides a more SoSA-centric approach to vehicle architectures by eliminating the need for a "bring your own antenna" mentality to the platform. But, most importantly, D3 provides a key affordable stepping stone approach for growing the Assured PNT strategy on vehicles platforms.

Technologies Affecting Assured PNT Strategy

Today's SAASM technology improves the integrity of the GPS signals received and utilized by the Warfighter. However, the path towards Assured PNT requires additional capability to improve this integrity and ensure mitigation of known and anticipated threats. What technology is on the doorstep that may complement D3 and improve PNT Assurance?



M-Code

A key component to the next generation of SAASM technology is the implementation of the USAF GPS Directorate's (GPSD) M-Code technology. M-code receivers, currently under development and test by three contractors to the GPSD, will be produced for munitions and airborne applications in addition to ground vehicle applications. Integrating an M-Code receiver to a device, such as D3, would be a no-nonsense approach to improving PNT data assurance by ensuring jam-resistant capability at a central

[3] Divis, Dee Ann. (2013, November 1). *Assured PNT: Army Links Smart Phones and GPS Devices*. InsideGNSS. Retrieved from http://www.insidegnss.com/node/3761

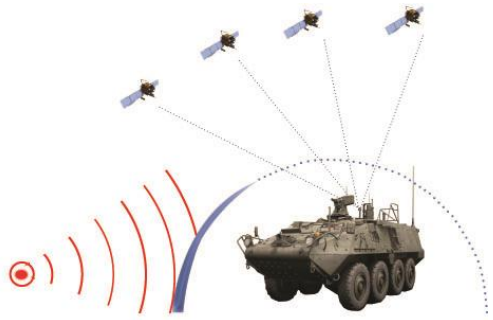
[4] Divis, Dee Ann. (2013, November 1). *Assured PNT: Army Links Smart Phones and GPS Devices*. InsideGNSS. Retrieved from http://www.insidegnss.com/node/3761

distribution point to all C4ISR onboard the platform.

M-code receivers will be integrated into the D3 and tested by the GPSD in FY14 and FY15. M-Code capable receivers will more effectively meet higher level PNT Assurance. Estimated by the Army's Product Director for PNT, upgrading fielded DAGRs and embedded GB-GRAMs to M-code capability would cost nearly 100% more than upgrading centralized D3 devices inside ground vehicles. This capability directly addresses a key requirement in the Assured PNT strategy.

Anti-Jam Antenna Technology

An immediate and available technology to protect against GPS jamming and spoofing is anti-jam antenna (AJ) technology. The most effective means of countering GPS interference and jamming is to include an active anti-jam (AJ) capability as an addition to a D3 device.



With the ability to create a null in the direction of the jammed or spoofed signal, an anti-jam antenna provides signal integrity to the receiver mounted inside the D3. Today's AJ antenna and receiver technology coupled with M-Code receivers are positioned to meet upper level PNT Assurance requirements.

Inertial Navigation Technology

Similar to anti-jam antenna technology, inertial navigation systems (INS) technology has matured over the past 5 to 10 years. The integration of GPS with INS offers significant anti-jam and other navigation performance benefits. INS can aid the GPS signal, allowing enhanced signal tracking sensitivity, detection of sophisticated spoofing, and hence provide more immunity to jamming. Possibly the most important factor when considering INS solutions for the ground vehicle platforms is affordability. Technology has developed over the past few years offering affordable price points for ground vehicle budgets and volumes. Whether considering a fiber optic gyro (FOG) or micro-electro mechanical (MEMS) INS solution, options are available for integration with D3, directly supporting Assured PNT requirements in ground vehicle architecture.

Timing Technologies

When GPS is completely denied by jamming, a major vulnerability is the loss of accurate timing signals from the GPS satellite constellation, referred to as 1 Pulse Per Second (1PPS). This accurate signal allows communications devices, such as tactical radios, to utilize encryption and electronic warfare devices to pinpoint IED threats. During extended durations of GPS denial, technology such as a Chip Scale Atomic Clock (CSAC), mated with a D3, can take over to maintain accurate timing data for hours or days at a time.

Figure 1 Chip Scale Atomic Clock developed by DARPA and commercially available through manufactures such as Symmetricom (35 grams total weight), offer affordable timing and sync capability on military vehicle platforms. [5]

With the help of DARPA and industry partners, small, accurate, and affordable timing and INS solutions are available to the ground vehicle community that can provide continuous heading and orientation data output for extended periods of time. Integration of a CSAC and/or INS with the

[5] U.S. Army Research, Development and Engineering Command (RDECOM) *Chip Scale Atomic Clock (CSAC)* Retrieved from http://www.armymantech.com/pdfs/CSAClock.pdf

D3 could directly address Assured PNT requirements.

Keys to Success

The key to the Assured PNT strategy will be to cost effectively integrate the aforementioned technologies into ground vehicle platforms. The centerpiece of this strategy is the DAGR Distributed Device (D3). Designing affordable navigation and timing systems to "plug and play" with D3 will provide the immediate infrastructure needed to support legacy C4ISR equipment onboard military vehicles in GPS denied environments.

D3 can function as the PNT distribution point of IS-GPS-153 PNT messages (working with M-Code and AJ) during normal GPS-based operations. In a true GPS denied environment, D3 could raise the level of PNT assurance by immediately "switching over" to distributed data off the INS. It would still continue to serve PNT data to FBCB2, JBC-P, tactical radios, navigation computers, fire control computers, airborne sensor links, or any C4ISR device. The transition would be seamless to the Soldier and last until normal GPS operations were restored. These technologies coupled with D3 could potentially meet the highest level of PNT assurance requirements. Most importantly, these levels of PNT assurance onboard a military ground vehicle could be achieved in today's budget constrained environment.

Conclusion

Once fielded, the D3 will serve as a key element in the support of Assured PNT for today's military ground vehicle fleet. Identifying, maturing, and integrating existing technologies to D3 are a direct path to achieve higher levels of PNT assurance for distribution within the ground vehicle architecture. This paper discussed the steps industry and government partners can follow to guarantee Assured PNT data is available to the systems integrators, platform managers, and most importantly, the Warfighter, now and into the future.