2017 NDIA GROUND VEHICLE SYSTEMS ENGINEERING AND TECHNOLOGY SYMPOSIUM
AUGUST 8-10 Novi, MICHIGAN

Enabling PNT Assurance at all Threat Levels

Mr. Aaron Mebust
Director of Product Management
GPS Source, Inc.
Pueblo West, CO

ABSTRACT

Global Positioning System (GPS) technology has become absolutely indispensable to today's warfighter. GPS signals provide Positioning, Navigation, and Timing (PNT) data that are needed by virtually every critical military system. Digital radio networks require precise time to operate. Direct and indirect fires systems need precise coordinates to accurately determine firing data. Individual soldiers and vehicles need positioning and navigation data to coordinate offensive and defensive maneuver. Battle management systems require the location of every friendly unit in order to provide commanders with an understanding of the battlefield. The list goes on and on. In short, PNT has become a critical element in the ability to shoot, move, and communicate. The dependency on PNT is well understood. The Secretary of the Army recently testified to Congress, "Having accurate PNT information is fundamental to our forces' ability to maintain initiative, coordinate movements, target fires and communicate on the move." (Coggins, 2016)

The most common source of PNT data is GPS. GPS is extremely cost effective, supporting unlimited users through its space based radio broadcasts. And, until recently, GPS has been universally available and has been a very reliable source of PNT. However, recent events have shown several world powers are in the process of re-invented land warfare. Certain state actors have revealing an advanced ability to disrupt precision navigation and timing capabilities (Australian Strategic Policy Institute, 2016). Our adversaries have increased their levels of sophistication and have attacked existing GPS capabilities with notable skill (Defense One, 2016). Global threats have questioned whether systems relying on PNT will work as expected on the modern battlefield. As Lt. Gen. H.R. McMaster shared in a recent brief, should the U.S. forces find themselves in a land war with Russia, they would be in for a rude, cold awakening (Defense One, 2016).

It is clear that an uninterruptable and reliable source of PNT is essential to the warfighter. It is also clear that solely relying on GPS is not a viable course of action for long term sustainability. Although GPS can be encrypted and the upcoming M-Code signals will be stronger, the inherent vulnerability of a weak, space based, sole source solution remains. Independent sources of PNT must be used for validation of GPS and generation of PNT when GPS is unavailable or untrusted. This capability, known as PNT Assurance provides an uninterrupted flow of reliable Positioning, Navigation, and Timing data. Today's warfighter needs PNT Assurance. Given our reliance on PNT and the vulnerability of GPS, PNT Assurance is not an option, it is a requirement.

Having said this, developing a PNT Assurance capability is much easier said than done. Formidable challenges present themselves in developing a solution that will detect threats to GPS, create accurate PNT in the absence of GPS, and then distribute valid PNT to all clients. Once the system is developed, fielding the solution will see challenges regarding integration into existing vehicle architectures along with the requirement to support legacy and future PNT clients. It will not be feasible to require replacement of every Command, Control, Communications, Computers, Intelligence, Surveillance, Reconnaissance and Electronic Warfare (C4ISR/EW) system in a modern vehicle to field a PNT Assurance capability. Finally,

ever present budget pressure will require a PNT Assurance solution that is cost effective, scalable, and upgradable. An expensive or "one size fits all" solution is not realistic.

When will this critically needed capability be available? Is it possible to move forward with existing vehicle architecture without waiting for new distribution methods (i.e., Ethernet VICTORY)? Can the U.S. and its NATO allies use currently available Commercial Off The Shelf (COTS) items to ensure PNT data accessibility no matter what the threat? Can the U.S. ensure adequate, authenticated PNT data regardless of GPS availability or integrity? Finally, how can cost effective fielding, scalability and sustainment be addressed?

This paper will address the challenge of developing a PNT Assurance capability. We will discuss the drivers and benefits using various sensors such as Chip Scale Atomic Clocks (CSAC), Inertial Navigation Systems (INS), and existing vehicle data sources such as a vehicle Controller Area Network (CAN) Bus to implement and field PNT Assurance. It will also discuss migrating to PNT Assurance while living within the constraints imposed by legacy systems that will never be completely updated. It will address the risks that must be mitigated and benefits achieved from a centralized PNT source distributing PNT to each client (a distributed architecture). Finally, this paper shall serve as a baseline recommendation to the ground vehicle community for bridging the gap between legacy systems deployed today and the C4ISR/EW architectures of the future by the distribution of valid PNT data across all formats (coaxial, wireless, serial data, Ethernet).

The conclusion supported shall be that a cost-effective strategy can be adopted by a joint industry/Government team for the implementation of PNT Assurance within an existing non-VICTORY architecture and that this solution shall support future VICTORY enabled architecture. The baseline PNT Assurance capability shall also serve as a proof of concept and a development platform for future developments in PNT resiliency.

Emergence of GPS

Achilles is the most famous hero of the Trojan War. Born of an immortal mother and human father, Achilles was dipped him into the river Styx shortly after his birth to make him immortal. However, since he was held by one heel, this spot did not touch the water and so remained mortal and vulnerable. Near the end of the Trojan War, Achilles was killed by Paris, who shot him in the heel with an arrow. From these legends, the term "Achilles heel" has come to mean a point of weakness, especially in a person or system that has no apparent vulnerabilities.

One could say that our military dependence on GPS makes it our Achilles heel. GPS is considered an indispensable military asset. It is the core navigation system for U.S. military aircraft, vessels, vehicles, and personnel. It has changed the nature of weapons targeting, command and control, guidance of unmanned systems, and battlefield logistics.

GPS has revolutionized the modern battlefield but "near-peer" adversaries are currently testing GPS denial technologies. Russia and China are investing heavily in both electronic and cyber warfare focusing on PNT. Electronic warfare can jam the signals carrying the data; cyber warfare can corrupt the data itself.

China, for instance, has been developing radar installations across artificial land created in the South China Sea. The installations expand the real-time domain awareness and ISR capabilities of the People's Liberation Army (PLA). These installations give PLA the capability to jam electronic sensor and radars in the region. PLA jamming includes denial of GPS, as exemplified by reports of their recent attempts to jam on-board equipment and GPS signals on the American Global Hawk UAV. (Australian Strategic Policy Institute, 2016)

Russia's ability to destroy command-and-control networks by jamming radio communications, radars and GPS signals, has been clearly

demonstrated in the Ukraine. Russia has significant resources devoted to electronic warfare (EW). These units conduct ground electronic attack, jamming communications, radar and command-and-control nets. (DefenseNews, 2015) Russia's advances in EW have been particularly noteworthy. Ukrainian separatist forces equipped with Russian EW systems have demonstrated a highly sophisticated ability to jam communications systems, deny access to GPS and interfere with the operation of sensor platforms. (Goure, 2017)

In June, 2017 more than 20 vessels in the Black Sea reported a GPS incident. US Coast Guard Navigation Center confirmed that GPS in the area at the time of the incident was within 3-meter accuracy. One ship's captain confirmed his GPS receiver appeared to be functioning normally, and was reporting a very accurate Horizontal Dilution of Precision (HDOP) with the indication that his position was "Safe within 100m". However, based on paper charts and radar, his actual position was 25 nautical miles away from the GPS reported position – near Gelendzhik Airport and more than a mile inland. The incident indicates bears all the attributes of a "spoofing" attack.

A GPS spoofing attack deceives a GPS receiver by broadcasting incorrect GPS signals, structured to resemble a set of normal GPS signals. The spoofed signals are typically modified in such a way as to cause the receiver to estimate its position or time to be incorrect, typically as determined by the attacker.

Even adversaries that are not necessarily "near peer" are challenging our military. In January of 2015, two U.S. Navy patrol boats wandered into Iranian waters. Ten U.S. sailors were captured and later released. US military officials seemed unable to explain how the U.S. Navy vessels had strayed from their intended path. Some have speculated that the Iranians conducted a spoofing attack by sending false GPS signals to lure the sailors into their territorial waters.

Spoofing may be considered even more dangerous than jamming. Jamming is easily detectible and reveals the presence of enemy forces. When done properly and as seen in the Black Sea incident, spoofing generates a false sense of security because all systems appear to be functioning properly during an attack. Spoofed GPS receivers can cause ground vehicles, airplanes, or ships to crash, or navigate into enemy territory. Spoofed receivers can also provide incorrect timing references, preventing computers and radio systems from functioning properly.

PNT Protection

More than a decade of persistent conflict has yielded significant advances in communications and battlefield-management tools fielded by US and allied forces. GPS technology has been implemented in areas never previously envisioned, including tactical radios, laptop computers, laser range finders, and smart phones. The introduction of SAASM capability in the early '90's significantly reduced the threat of spoofing or jamming of the GPS frequencies, further enabling these beneficial applications.

The Defense Advanced GPS Receiver (DAGR) was introduced by Rockwell Collins in 2004. The DAGR brought secure encryption to the soldier level. To date, over 400,000 DAGR's have been fielded to ground vehicles and individual soldiers and the DAGR is a critical element of PNT security. In most cases, the DAGR provides a secure GPS message (ICD-GPS-153 protocol) to a PNT client, such as a tactical radio or MFOCS computer. Other systems realized SAASM compliance by embedding a single GB-GRAM GPS receiver in their design. For vehicles with multiple PNT clients, each device required its own GB-GRAM or DAGR. In a case study of the US Army's Stryker Commander Vehicle, up to three tactical radios, an onboard navigation computer, electronic warfare device, and remote weapon station all require secure PNT information. These seven clients required support from seven individual DAGR's and GB-GRAM's. A "stovepipe" architecture resulted in

each client having its own antenna or GPS splitter. Although SAASM protection was delivered to PNT client systems, the acquisition and installation costs proved to be prohibitive and the costs to upgrade were extreme.

In June 2012, GPS Source began development of a new low-cost, secure GPS PNT signal distribution hub. Developed entirely with private funds, the DAGR Distributed Device (D3) had the ability to replace up to four DAGRs within a ground vehicle platform. It eliminated the need for multiple DAGR devices, embedded GB-GRAM receivers, and multiple antennas. The D3 uses a single GB GRAM and a single antenna to provide PNT to up to eight clients (two per DAGR port). Upgrading the D3 resulted in improved protection to all vehicle clients simply by touching one device. This approach, distributed architecture, proved to be an affordable, sustainable and realistic approach to providing the Warfighter with secure PNT information. In a declining budget environment, the D3 offered a huge benefit to platform managers, platform operators & maintainers. It also provided systems integrators with a means to more efficiently distribute secure GPS data within the confines of their vehicles.

Programs Under Development

Although the US military is working towards programs that will address electronic support/electronic protection capability (ESEP), equipment currently fielded has not been designed with address today's significant electronic attack capabilities. The Defense Advanced Research Project (DARPA) has several programs focused on PNT that will decrease reliance on GPS. These technologies include micro-technology, adaptable navigation systems, and projects such as Special, Temporal and Orientation Information in Contested Environments (STOIC) (DARPA, 2014). However, all these efforts are currently in the conceptual stage with very long development cycles and successful conclusion is not guaranteed.

One developing U.S. Army Program of Record, Assured PNT (A-PNT) intends to utilize a multiple sensors and an open architecture to create an integrated Assured PNT solution that is resilient and easy to update. However, the A-PNT Program of Record is several years away from Initial Operational Capability (IOC) and it may be several years after IOC before a full fielding effort can bring this solution to troops in the field.

When looking at "near peer" adversary cycle times, the U.S. can see their adversary's agility and focus gives them plenty of opportunities (i.e. time) to field counters to our capabilities. (Mabbett & Kovach, 2017) The short cycle time of our adversaries will require us to field interim solutions on a much more rapid timeframe, potentially building on those interim solutions and using lessons learned to develop an even more capable solution.

Requirements Summary for PNT Protection

The first step in addressing a system that will deliver comprehensive PNT protection is to first define all requirements and constraints. A secure, resilient PNT would have the capability to formulate and distribute reliable, accurate, trusted and unhindered PNT data to platform C4ISR/EW systems from a centralized source. It would do so in a manner that ensured the systems' dependency on PNT could not be exploited by the enemy, and provide unhindered access to trusted PNT information under all conditions, including times when space-based PNT may be limited, denied, or rendered suspect by an adversary.

A Secure, Resilient PNT Solution would include all of the following attributes:

1. **Encrypted Signal Support**

One of the most important PNT sensors in PNT Assurance systems is the GPS receiver. Jamming GPS signals is a simple but effective method to deny GPS. However, a more sinister threat comes from systems that transmit false GPS/GNSS signals that result in incorrect

readings for Positioning Navigation and Timing. The current method for addressing these spoofing attacks is to encrypt GPS/GNSS signals. The PNT Assurance solution must be capable of accommodating today's SAASM receiver cards capable of decryption and must be able to accommodate receiver cards that will be available in the future (i.e., M-Code).

2. Sensor Integration

An effective PNT Assurance solution must successfully integrate various PNT sensors in a unified manner, enabling Electronic Surveillance/Electronic Protection (ES/EP) applications to effectively utilize all sensor data to detect the presence of threats to space-based PNT signals. The ES/EP application must deliver a trusted, accurate, and uninterrupted source of PNT data to the platform's C4ISR/EW suite. The ES/EP applications must be easily upgradeable on fielded platforms to immediately counter the introduction of new threats in the Area of Responsibility (AOR) and to exploit the evolution of new PNT sensor technologies.

3. PNT Distribution

In modern military platforms, the PNT Assurance solution must not only support legacy IS-GPS-153 and IS-GPS-164 compliant systems, but it must also be fully compliant with Ethernet standards currently being developed such as Vehicle Integration for C4ISR/EW Interoperability (VICTORY). The PNT Assurance system must support the applicable Ethernet component types and fully integrate with Ethernet switching and platform computing resources. It is important to note that the PNT Assurance capability should not be confused with the vehicle's Ethernet hub, router, or switch. The PNT Assurance capability is simply a Generic End Node device and the network time source (NTP or PTP IEEE1588). The PNT Assurance capability can also serve as the Ethernet to Serial adapter.

4. Scalability

A well-designed solution for ground vehicle and aircraft platforms must be scalable. Some platforms may require only a basic level of PNT distribution while others will require more extensive capabilities. Should missions, funding, or threats require changing the existing capability of a specific vehicle, the PNT Assurance solution should be easily modified to meet the new requirements.

5. Upgradeability

The most significant requirement of the PNT Assurance design is to have an open, scalable architecture that can grow with technology to pace future threats. An open, standardized architecture allows these and other future sensor technology to be integrated into the PNT Assurance solution.

6. Monitor & Control

Confirmation of the integrity of the PNT data is a critical requirement for a PNT Assurance solution. The PNT Assurance system must have the ability to independently assess the validity of the PNT data that it distributes to the host platform, and effectively communicate this assessment to the system operators.

7. Ruggedized Military Design

The PNT Assurance system must satisfy the requirements of applicable Military Standards, such as MIL-STD-810, MIL-STD-461, and MIL-STD-1275/704. The PNT Assurance solution must be optimized for Size, Weight, Power, and Cost (SWaP-C).

8. Cost Effectiveness

Vehicle upgrades must have the capability of integrating into existing architectures and must be designed to accommodate future vehicle architectures, such as VICTORY. A well-designed PNT Assurance architecture will allow for installation of a cost effective basic capability and allow for rapid upgrades in the future.

Delivering Tomorrow's Solution Today

So now that we have defined the need and the proposed response time, what if industry collaborated and produced a group of modular

solutions that would deliver accurate PNT data even if GPS was not available for a significant period? What if they made it cost effective, accessible, distributed and easy to integrate with legacy and future technology? What if the challenges of evolving into the desired solution while living within the constraints imposed by the legacy systems was addressed? What if the challenges of Space, Weight, Power, and Cost was considered? And what if it was available now?

GPS Source and its partners have developed just such a system. This solution, called ***SENTRySCOUT***, is a resilient positioning, navigation and timing system, providing trusted and reliable PNT data to C4ISR/EW clients in Ethernet and IS-GPS-153 formats to Ethernet and Serial clients whether or not GPS is available.

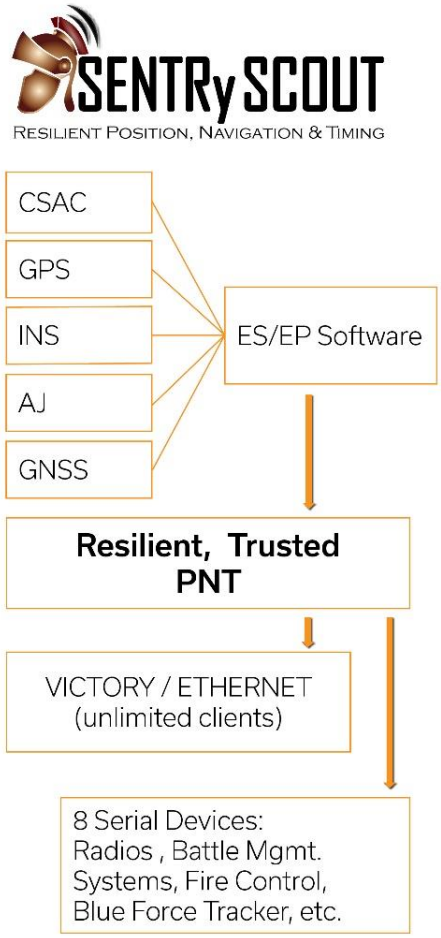

Figure 1 ***SENTRySCOUT*** *Resilient Position, Navigation & Timing System*

The ***SENTRySCOUT*** system incorporates the following:

1. M-Code & SAASM GPS compatible Enhanced DAGR Distributed Device (ED3)
2. VICTORY/CSAC Accessory Module (VCAM), which includes:
   - A Chip Scale Atomic Clock (CSAC)
   - An Inertial Navigation System Interface
   - Dual GNSS Receivers
   - An Automotive CAN 2.0b Interface
   - An Ethernet Data Bus Interface
3. Electronic Support/Electronic Protection software from Talen-X, Broadshield™ for detection, monitoring, reporting
4. A GNSS receive antenna
5. The Raytheon *Landshield* Anti-Jam Antenna which mitigates jammer effectiveness
6. The high-performance *TACNAV 3D* Inertial Navigation System from KVH

It is important to note that the sensors in the ***SENTRySCOUT*** *R-PNT* System can be selected to meet the requirements of the user. For example, a high grade INS can be used when precise positioning data is required. Or, a low grade INS can be used for vehicles with lower mission requirements. Or, if a vehicle already has an on-board INS, that existing INS can be integrated into the ***SENTRySCOUT*** *R-PNT* System to reduce cost and eliminate additional components inside the vehicle. Varying types of AJ Antennas provide different levels of jammer protection and can deliver varying types of information to the battlefield commander. Similarly, the ES/EP software can be upgraded or replaced with another monitor and control application in response to emerging threats and the resulting mitigation measures.

Enhanced DAGR Distributed Device (ED3)

The foundation of the ***SENTRySCOUT*** *R-PNT* System is the Enhanced D3 (ED3). The ED3 is an improved version of the original DAGR Distributed Device (D3). The ED3 uses a single GPS receiver card to provide IS-GPS-153 messages to up to eight separate clients. When development efforts are complete, the ED3 will be able to accommodate either a SAASM capable GB-GRAM or an M-Code GB-GRAM-M. The ED3 is an example of distributed architecture to deliver PNT to C4ISR/EW systems. A distributed architecture is critical to reducing costs for future system upgrades because it allows a user to upgrade a single central hub to have all system clients receive the benefits of the upgrade. In contrast, the stovepipe architecture common to most vehicles requires the user to upgrade each client separately to upgrade the capability of the entire vehicle.

Figure 2 Enhanced DAGR Distributed Device (ED3)

The ED3 is the US Army's Lead Platform for M-Code implementation. The ED3 configured with SAASM GPS has received Security Approval from the USAF GPS Directorate. Security Approval for Enhanced D3 configured with M-Code GPS is anticipated in February 2018.

The diagram below shows a notional Enhanced D3 installation where four separate PNT clients are supported by an ED3 hosting a single GB GRAM receiver card.

Figure 4 ED3 Notional Installation

ED3 PNT Assurance Compatibility

GPS Source has incorporated two important capabilities that provide the foundation for a PNT Assurance: Anti Jam Antenna Integration, and an PNT Assurance accessory interface.

1. Anti-Jam Antenna Support

Anti-Jam (AJ) antennas provide significant benefits to the user in a jammed environment. By steering nulls towards jamming sources, AJ antennas can provide GPS signals in environments that would otherwise overwhelm unprotected receivers.

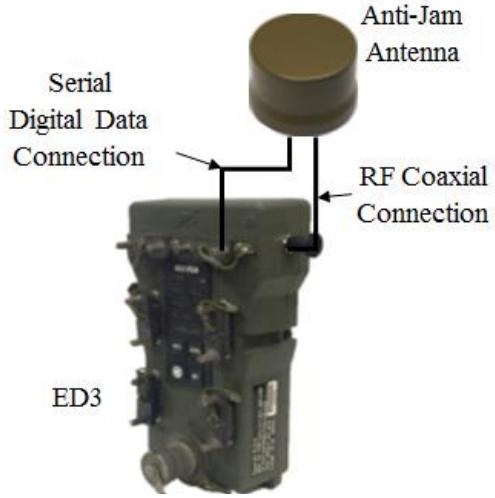

Figure 3 Enhanced D3/AJ Antenna Connections

The ***SENTRySCOUT*** *Resilient PNT System* is being designed to operate with industry standard Fixed Radiation Pattern Antennas (FRPA) as well as Anti-Jam (AJ) antennas that provide a significant reduction in interfering signals. GPS Source is closely coordinating the design of the ***SENTRySCOUT*** *R-PNT System* with industry leaders in Anti-Jam Antenna technology to fully integrate the AJ Antenna functionality. This results in system capabilities that are far beyond the benefits of reduced interfering signal levels.

AJ antennas with digitally processed signals feature numerous advantages over analog implementations. Specifically, digital AJ antennas feature serial data interfaces that enable host platform applications to interface with the antenna, monitoring and controlling antenna operational modes (e.g. enabling operation with pseudolites), retrieving antenna performance and fault data and capturing data pertaining to the electromagnetic threat (i.e. enhanced situational awareness). The ***SENTRySCOUT*** *R-PNT System* will include a serial data interface that connects to compatible AJ antennas which will enable the system software to optimize the AJ antenna vehicle integration, providing a significant performance enhancement over simply connecting to the RF output of the antenna.

Furthermore, antenna mode and delay information can be used for ensuring compatibility with pseudolites (per IS-GPS-250A, P(Y)-Code External Augmentation System).

Additionally, AJ Antennas provide information regarding the presence of a jammer. This information is critical to the ES/EP software when assessing the integrity of the GPS data. This assessment can be used to prevent corruption of the inertial navigation and system clock filters, as well as meeting any requirement for reporting of PNT data integrity.

An effective PNT Assurance solution design must utilize the advantages of a fully integrated digital AJ Antenna and be capable of realizing more from the antenna than just reduction of the interfering signals. The ***SENTRySCOUT*** *R-PNT System* is designed to do exactly that.

2. PNT Assurance Accessory Interface

The Enhanced D3 includes a connector on the back panel that allows for installation of a PNT Assurance capable device. This device, the VICTORY/CSAC Accessory Module (VCAM), described below, allows for integration of multiple sensors which allow for a true PNT Assurance capability.

VICTORY/CSAC Accessory Module for the Enhanced D3 (VCAM)

The VCAM is a highly compact PNT Assurance accessory module that mounts to the back of the Enhanced D3. The Enhanced D3 with VCAM will provide the host platform's C4ISR/EW suite with unhindered access to accurate, trusted PNT data delivered to both the vehicle's Ethernet data bus and all vehicle clients with serial data interfaces compliant to IS-GPS-153. The Enhanced D3 with the VCAM installed retains 100% compatibility with all standard DAGR mount accessories and does not expand the X/Y space claim or Z axis intrusion of the Enhanced D3 beyond the original space claim/intrusion of the D3 or DAGR.

Figure 5 Enhanced D3 with VCAM in DAGR Mount

Adding the VCAM to the Enhanced D3 enables:

1. Resilient time capability based on the VCAM's CSAC module
2. Integration of an inertial navigation system such as the KVH *TACNAV 3D*

3. ES/EP capability with the Talen-X, Inc. "Broadshield" ES/EP application
4. Ethernet interface to the host platform

In short, the Enhanced D3 with VCAM allows for the implementation of a full position, navigation, and timing assurance capability of the ***SENTRySCOUT*** system.

VCAM GNSS Receivers and ES/EP

The VCAM includes two Global Navigation Satellite System (GNSS) chip scale receivers. The GNSS receivers are not used to provide PNT data to the host platform. Currently, the only receiver used as a source for reference PNT data is the Enhanced D3's SAASM or M-Code GPS.

The GNSS receivers will be leveraged by the VCAM's ES/EP algorithms as L-band sensors to detect and identify threats, thereby assessing the vulnerability of the military GPS receiver. While the Enhanced D3's SAASM or M-Code receiver is providing PNT using encrypted military signals (P(Y) or M-Code), the GNSS receivers will be used by the ES/EP software to monitor and observe the impact of the jamming on other GNSS signals. The GNSS receivers can also act as a calibration source for the AJ Antenna delay during benign conditions (e.g. when the absence of jamming is confirmed).

VCAM Timing Reference System

The VCAM will include a precise time reference in the form of a Chip Scale Atomic Clock (CSAC). The CSAC will be disciplined by GPS signals as long as GPS is determined to be valid. When GPS is not available or has been determined to be invalid, the CSAC will not be disciplined and will become the time reference for the clients attached to the Enhanced D3. The CSAC can also be used as an IEEE 1588 time source for all Ethernet clients (when Ethernet functionality has been developed). GPS Source anticipates the CSAC will provide precise time to within 1 µs of UTC for up to 8 hours in a GPS-denied environment.

VCAM Ethernet Capability

The VCAM features an integrated Ethernet capability through a miniature IP-67 rated connector. The VCAM can be delivered with a 6 in. to 8 in. adapter cable that will adapt the miniature connector of the VCAM to a MIL-D-38999 connector that is compliant with the ATPD-2410 specification for Ethernet cables, 10 Megabit to 1 Gigabit per second. Ethernet functionality will be complete by the end of CY 2017 with VICTORY protocol capability in 2018.

VCAM Future Non-GPS Navigational Aid Upgrades

The GPS Source VCAM solution for the PNT Assurance system is designed with an open architecture Application Programming Interface (API) that enables GPS Source or any other 3rd party to upgrade the capabilities of the VCAM as technologies evolve. For example, the INS interface is fully defined within an open Interface Control Document (ICD). With further development, PNT data from a visual cued navigation system can be routed to the Enhanced D3/VCAM and fused with data from the INS to enhance the system's navigation performance. Furthermore, with the future integration of a Signal of Opportunity receiver, pseudo-range data to other electromagnetic emitters (e.g. Iridium, eLoran, etc.) for which the location is precisely known can significantly increase the robustness of the navigation capability, greatly reducing the dependency on GPS.

VCAM Development Timeline

Initial deliveries of the VCAM are scheduled for October 2017. Initial deliveries will provide a precise time reference capability, a limited ES/EP function, and the ability to integrate certain INS and AJ antenna systems. Initial deliveries in September will not include Ethernet functionality. Ethernet capabilities are currently scheduled for the end of calendar year 2017.

Inertial Navigation System

The ***SENTRySCOUT*** is available with an Inertial Navigation System (INS) manufactured by KVH Industries, Inc. Future expansion includes the option of using Inertial Navigation Systems from different manufacturers (i.e., GE Aviation, L3, Honeywell, Kearfott) for vehicles already equipped with an INS.

Figure 6 KVH TACNAV 3D Engine Inertial Navigation System

GPS Source has included KVH's *TACNAV 3D*, ultra-high performance, ultra-compact INS at a price that is unprecedented for equivalent performance. The *TACNAV 3D* has been fielded to multiple militaries in more than a dozen countries with over 21,000 units fielded.

The *TACNAV 3D* features high-performance navigation filters and sensor inputs from the VCAM's CAN2.0b bus (i.e. odometer, tire inflation, etc.) and KVH's high-performance Fiber Optic Gyroscope (FOG) inertial measurement units (IMUs). Employing KVH's latest developments in tactical inertial navigation technology, the *TACNAV 3D* provides extremely accurate heading (0.05° with GPS), dead reckoning navigation (0.2% of distance traveled) and orientation. The *TACNAV 3D* combined with the GPS Source ED3/VCAM delivers reliable position and navigation data in GPS-denied environments with greater accuracy and at a lower cost than any competing navigational system of similar performance.

Electronic Support/Electronic Protection Software

The Electronic Support/Electronic Protection (ES/EP) application monitors, records, and ensures the validity of the PNT solution generated from the Enhanced D3/VCAM and external INS. The ES/EP application provides PNT Assurance by analyzing sensor data and determines the validity and accuracy of the data. Various send data to the ES/EP software engine. Sensor data is processed through a matrix of algorithms that can instantly detect environments with malicious data, deceptive signals, and RF jamming. If a threat is detected, the ES/EP software immediately takes mitigation actions to ensure downstream devices are not compromised.

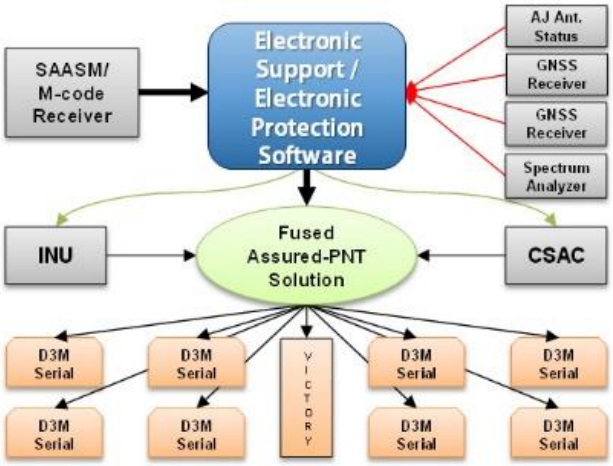

Figure 7 Electronic Support/Electronic Protection Integration

The integration between the sensors and the ES/EP software is seen in the ES/EP software integration figure above. In accordance with the guidance provided in DoD Instruction 4650.08 Positioning, Navigation, and Timing (PNT) and Navigation Warfare (Navwar) dated February 5th, 2015, the only source of PNT used by the

Recording malicious events for post-mission analysis and characterization provides an essential basis for Blue Force counter measures on future missions. The software may be configured for continuous logging or triggered logging (i.e. only log data when a threat is detected) to minimize storage usage.

With the ***SENTRySCOUT*** ES/EP software detecting jammer environments and preventing invalid data from corrupting the Kalman predictive filters of the on-board CSAC oscillator

and the tightly coupled *TACNAV 3D* INS, the ***SENTRySCOUT*** system can be trusted to provide uninterrupted valid PNT, even in degraded and denied GPS environments. It facilitates the ability for soldiers to carry out their mission in electronic warfare (EW) situations while maintaining accurate timing for communication and accurate position for navigation.

Summary:

Threats to GPS exist and the implications of PNT denial are significant. Denial of GPS will result in the ability of the warfighter to shoot, move, and communicate. Not only will mission success be at risk, but the warfighters themselves will be exposed to greater danger. Inaction on this issue is not an option.

Industry leaders have shown that critical needs such as the threat to PNT can be addressed quickly and cost effectively by partnering. The result of such a partnership in this instance has led to the development of a scalable and upgradable system that defeats threats to GPS and will assure the flow of reliable and trusted PNT to all C4ISR/EW clients, both legacy and future. Further testing and integration will be required to confirm and field a solution, but it is clear that a solution exists today that can address this critical threat today and well into the future.

References

Australian Strategic Policy Institute. (2016, August 24). *Electronic Warfare in the South China Sea.* Retrieved from The Strategist: https://www.aspistrategist.org.au/electronic-warfare-south-china-sea/

Coggins, K. (2016, August 29). *Acquisition Reform Baked-In.* Retrieved from Acquisition Reform Baked-In: https://www.army.mil/article/174190/acquisition_reform_baked_in

DARPA. (2014, July 24). *Beyond GPS: 5 Next-Generation Technologies for Positioning, Navigation & Timing (PNT).* Retrieved from www.darpa.mil: http://www.darpa.mil/news-events/2014-07-24

Defense One. (2016, October). *How the Pentagon is Preparing for a Tank Ware With Russia.* Retrieved from www.defenseone.com: http://www.defenseone.com/assets/future-land-warfare-ebook/portal/

DefenseNews. (2015, August 2). Retrieved from DefenseNews.com: http://www.defensenews.com/story/defense/policy-budget/warfare/2015/08/02/us-army-ukraine-russia-electronic-warfare/30913397/

Goure, D. D. (2017, January). *Army-Modernization.* Retrieved from lexingtoninstitute.org: http://lexingtoninstitute.org/wp-content/uploads/2017/01/Army-Modernization.pdf

Mabbett, A., & Kovach, J. (2017, January). *"Third Offset" Strategy Calls for Fresh Thinking.* Retrieved from NationalDefenseMagazine.org: http://www.nationaldefensemagazine.org/archive/2017/January/Pages/ThirdOffsetStrategyCallsforFreshThinking.aspx

Smithsonian. (2017, January). *Time and Navigation, The untold story of getting from here to there.* Retrieved from timeandnavigation.si.edu: https://timeandnavigation.si.edu/satellite-navigation/gps