Defense Systems Information Analysis Center

DSIAC TECHNICAL INQUIRY (TI) RESPONSE REPORT

Assured Positioning, Navigation, and Timing (APNT)

Report Number:
DSIAC-BCO-2021-163
Completed January 2021

DSIAC is a Department of Defense Information Analysis Center

MAIN OFFICE
4695 Millennium Drive
Belcamp, MD 21017-1505
443-360-4600

REPORT PREPARED BY:
Dr. Craig Arndt
Office: QinetiQ

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
18-01-2021	Technical Research Report	

4. TITLE AND SUBTITLE:

Assured Positioning, Navigation, and Timing (APNT)

5a. CONTRACT NUMBER
FA8075-21-D-0001

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S):

Dr. Craig Arndt

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Defense Systems Information Analysis Center (DSIAC)
QinetiQ
10440 Furnace Rd Suite 204
Lorton, VA 22079

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Defense Technical Information Center (DTIC)
8725 John J. Kingman Road
Fort Belvoir, VA 22060-6218

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Distribution A. Approved for public release: distribution unlimited.

13. SUPPLEMENTARY NOTES
Space: positioning, navigation, and timing (PNT); command, control, communications, computers, and intelligence (C4I): networks and communication; Military Sensing

14. ABSTRACT
The U.S. Armed Forces have become reliant on the Global Positioning System (GPS) for precision navigation for foot mobile infantry to high-end precision weapons. Assured positioning, navigation, and timing (APNT) is defined as the ability to provide operational forces continuous access to position, velocity, attitude, and time information with confirmed integrity and sufficient accuracy to perform their mission under the complete range of threat conditions. Threat conditions include, but are not limited to, GPS degradation, denial, and deception. This report examines several aspects of APNT and its threats and describes many of the ongoing APNT programs within the U.S. Department of Defense and several of the major defense contractors' research and development projects.

15. SUBJECT TERMS
assured positioning, navigation, and timing (APNT); positioning, navigation, and timing (PNT); Global Positioning System (GPS); GPS denial; GPS degradation; GPS deception

16. SECURITY CLASSIFICATION OF: U			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			Ted Welsh, DSIAC Director
U	U	U	UU	20	**19b. TELEPHONE NUMBER** *(include area code)* 443-360-4600

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39.18

ABOUT DTIC AND DSIAC

The Defense Technical Information Center (DTIC) preserves, curates, and shares knowledge from the U.S. Department of Defense's (DoD's) annual multibillion dollar investment in science and technology, multiplying the value and accelerating capability to the Warfighter. DTIC amplifies this investment by collecting information and enhancing the digital search, analysis, and collaboration tools that make information widely available to decision makers, researchers, engineers, and scientists across the Department.

DTIC sponsors the DoD Information Analysis Centers (IACs), which provide critical, flexible, and cutting-edge research and analysis to produce relevant and reusable scientific and technical information for acquisition program managers, DoD laboratories, Program Executive Offices, and Combatant Commands. The IACs are staffed by, or have access to, hundreds of scientists, engineers, and information specialists who provide research and analysis to customers with diverse, complex, and challenging requirements.

The Defense Systems Information Analysis Center (DSIAC) is a DoD IAC sponsored by DTIC to provide expertise in 10 technical focus areas: weapons systems; survivability & vulnerability; reliability, maintainability, quality, supportability, and interoperability (RMQSI); advanced materials; military sensing; autonomous systems; energetics; directed energy; non-lethal weapons; and command, control, communications, computers, intelligence, surveillance, & reconnaissance (C4ISR). DSIAC is operated by SURVICE Engineering Company under contract FA8075-21-D-0001.

A chief service of the DoD IACs is free technical inquiry (TI) research, limited to 4 research hours per inquiry. This TI response report summarizes the research findings of one such inquiry jointly conducted by DSIAC.

ABSTRACT

The U.S. Armed Forces have become reliant on the Global Positioning System (GPS) for precision navigation for foot mobile infantry to high-end precision weapons. Assured positioning, navigation, and timing (APNT) is defined as the ability to provide operational forces continuous access to position, velocity, attitude, and time information with confirmed integrity and sufficient accuracy to perform their mission under the complete range of threat conditions. Threat conditions include, but are not limited to, GPS degradation, denial, and deception. This report examines several aspects of APNT and its threats and describes many of the ongoing APNT programs within the U.S. Department of Defense and several of the major defense contractors' research and development projects.

Contents

List of Figures

1.0 TI Request

1.1 INQUIRY

What U.S. Department of Defense (DoD) and defense contractor research or programs address assured positioning, navigation, and timing (APNT)?

1.2 DESCRIPTION

The approach areas of interest include the following:

- Positioning, Navigation, and Timing (PNT) Source Selection: Enables the operator to include or exclude discreet PNT sources.
- PNT Source Abstraction: Translates PNT source data and metadata into a standard interface protocol, separating the specific sensor implementation from the downstream data processing.
- Navigation Functions: Derive PNT data or metadata from one or more core or exploitable sensors.
- Integrity Algorithms: Route PNT source data and metadata through the appropriate set of integrity fault and information assurance fault detection algorithms.
- Fault Extraction: Functions that discriminate and exclude PNT source data and metadata based on integrity thresholds defined in integrity algorithms.
- Data Fusion: Functions that instantiate state estimation algorithms, e.g., Kalman Filter, Extended Kalman Filter, Unscented Kalman Filter, Rao-Blackwellized Particle Filter, etc.
- PNT Propagation: Function that translates and distributes assured or unprocessed position, velocity, attitude, or time data and metadata into native PNT consumer interfaces.

2.0 TI Response

2.1 PNT

PNT is a combination of the following three distinct capabilities [1]:

1. **Positioning**. The ability to accurately and precisely determine one's location and orientation two-dimensionally (or three-dimensionally when required) referenced to a standard geodetic system (such as World Geodetic System 1984).
2. **Navigation**. The ability to determine current and desired position (relative or absolute) and apply corrections to course, orientation, and speed to attain a desired position anywhere around the world, from subsurface to surface and from surface to space.

3. **Timing**. The ability to acquire and maintain accurate and precise time from a standard (Coordinated Universal Time, or UTC) anywhere in the world and within user-defined timeliness parameters. Timing also includes time transfer.

When PNT is used with map data and other information (e.g., weather or traffic data), the result is the most popular and recognizable service—the modern navigation system better known as the Global Positioning System (GPS).

The U.S. National PNT Architecture (Figure 1) is managed by the U.S. Department of Transportation. Although GPS and PNT were developed by the DoD, they are now mostly used outside of the DoD for a wide range of location and tracking applications. However, different parts of the DoD continue to use GPS and PNT technologies extensively. The military's use of PNT is, in many cases, different than nonmilitary use. In addition, the military's use of PNT systems faces the challenge of hostile forces attacking the capabilities created by high-quality PNT [1].

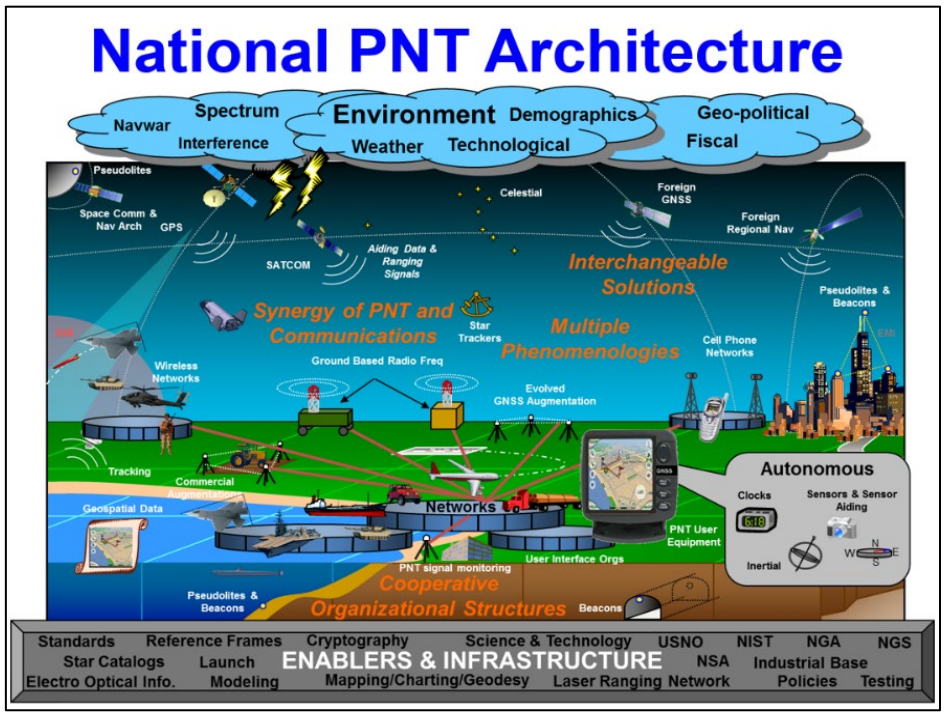

Figure 1: National PNT Architecture [1].

The military's use of PNT is not limited to simple navigation but can include targeting opposing forces and weapons systems as well as locating friendly forces.

The potential vulnerabilities of the military's dependence on GPS and Global Navigation Satellite System (GNSS) data are driving demand for new deployed approaches for detecting threats. In GPS/GNSS-denied environments, ensuring that accurate PNT information is

delivered to the Warfighter is critical. APNT is therefore essential to the DoD in any environment to ensure the continued use of the U.S. military's full range of defensive and offensive capabilities.

2.2 THREATS TO PNT

The enemies and opponents of the United States and its military have recognized PNT as a key technology to attack as part of integrated attacks against U.S. capabilities and forces. Threats to PNT can be categorized into the following three major groups based on their impact on the PNT or GPS systems:

1. **GPS Signal Degradation.** If an enemy can degrade GPS signals, then the accuracy and/or the reliability of the GPS system that enables the PNT is adversely impacted, and DoD systems and forces cannot perform their missions. There are several different technologies that can be used to degrade GPS signals.
2. **GPS Denial Systems.** These systems primarily use jamming systems to prevent DoD systems from receiving GPS data for PNT applications.
3. **GPS Deception.** The enemy tries to spoof GPS system inputs to provide the DoD systems with false PNT data, which significantly degrades the performance of those systems.

2.3 APNT APPLICATIONS IN WEAPONS SYSTEMS

How APNT is implemented within existing DoD weapons systems is a complex topic and area of development. Some of the key topics in APNT applications are discussed in Sections 2.3.1 through 2.3.7.

2.3.1 PNT Source Selection

PNT source selection enables the operator to include or exclude discrete PNT sources. To increase the overall performance of the PNT functions in each system, there may be more than one source of PNT data. In most cases, there will be a GPS source and then there may be one or more other sources, including sensor systems and/or internal navigation systems (INSs). By dynamically selecting different sources, systems can improve their PNT performance and resilience to counter PNT threats.

2.3.2 PNT Source Abstraction

PNT source abstraction translates PNT source data and metadata into a standard interface protocol, separating the specific sensor implementation from the downstream data processing. With the standardization of the different data, PNT data and metadata will be easier to aggregate and use advanced signal processing tools.

2.3.3 Navigation Functions

Navigation functions derive PNT data or metadata from one or more core or exploitable sensors. Navigation is a critical function for all military applications and requires knowledge of location, direction, and speed. Reliable and accurate PNT data allow the vehicles and systems to travel as needed to perform their missions.

2.3.4 Integrity Algorithms

PNT source data and metadata are routed through the appropriate set of integrity fault and information assurance fault-detection algorithms. In hostile, GPS-threatened environments, integrity algorithms are used to both validate the quality and reliability of PNT data and data sources and detect different types of spoofing activities from adversaries.

2.3.5 Fault Extraction

Fault extraction involves functions that discriminate and exclude PNT source data and metadata based on integrity thresholds defined in integrity algorithms. The purpose of fault extraction is to determine the reliability of PNT data in an organized manner. If the data are unreliable for any reason, then they can be disregarded and other data from different sources can be used.

2.3.6 Data Fusion

Data fusion involves functions that instantiate state estimation algorithms (e.g., Kalman Filter, Extended Kalman Filter, Unscented Kalman Filter, Rao-Blackwellized Particle Filter, etc.). Data fusion systems use a wide range of different algorithms to use two or more data sources at the same time. Generally, two or more data sources can be combined to get a more reliable and accurate reading than by relying on a single source of data.

2.3.7 PNT Propagation

PNT propagation involves functions that translate and distribute assured or unprocessed position, velocity, attitude, or time data and metadata into native PNT consumer interfaces. In addition to general propagation, there are other ways PNT data can get to the systems that need the data, one of which the DoD is most interested in—point-to-point communications. With secure communication links, PNT data can be shared between different systems within a secure network, mitigating hostile PNT/GPS jamming or deception and providing the data, as needed, from a secure source.

Many of the APNT technologies and approaches are based on using alternative means of navigation and timing besides GPS. Because the military cannot rely on GPS in contested environments, the DoD is pursuing alternate technologies. Interestingly, some of these technologies, including INSs and map-matching technologies, existed before GPS and are now being reexamined for APNT applications.

2.4 DoD PROGRAMS

The DoD continues to develop its programs in PNT, GPS, and APNT. In addition, the DoD and the U.S. Congress have mandated significant policy regarding PNT [2]:

> The U. S. Congress, especially the Armed Services Committees, have long been concerned about GPS and PNT issues. Over the last two decades Congressional hearings, demands for reports, and investigations have dealt with acquisition, contingency plans for when space is not available, deliberate interference, and a host of other issues. While these actions all evidenced Congress's interest and concern, they were relatively passive measures.

However, in 2018 the National Timing Resilience and Security Act was passed, which required the Department of Transportation to establish a terrestrial timing system to back up GPS signals. Then in 2019, Congress appropriated money for a GPS Backup Technology Demonstration. The National Defense Authorization Act (NDAA) for 2020 required the Air Force to develop a prototype multi-GNSS receiver as part of its resiliency efforts. The NDAA for 2021 also reflects Congress's transition to an active player in national PNT issues and policy, including the following provisions [2]:

> The 2018 NDAA required the Defense Department to incorporate Europe's Galileo and Japan's QZSS satellite navigation signals into military user equipment. The idea was to make it more resilient to disruption. Also required was an investigation into using non-allied signals.
>
> Apparently not satisfied with progress on this project, Congress mandated a project to develop a prototype multi-GNSS receiver as part of the 2020 NDAA.

In the 2021 NDAA, Congress withheld 20 percent of the funding for the Office of the Secretary of the Air Force until the Air Force certified that the prototype multi-GNSS receiver project was underway and the Air Force provided briefings to the Senate and House Armed Services Committees.

Section 1611 of the Act is titled "Resilient and Survivable Positioning, Navigation, and Timing Capabilities." It requires development, integration, and deployment of these capabilities for combatant commanders within two years. This requirement is "… consistent with the timescale applicable to joint urgent operational needs statements…" [2]. The Act also states that the new PNT capabilities shall "generate resilient and survivable alternative positioning, navigation, and timing signals" and "process resilient survivable data provided by signals of opportunity and on-board sensor systems."

The Act reverses the DoD's 2018 PNT Strategy's plan for future systems to be classified and for military use only. It directs the DoD to work with the National Security Council, Departments of

Transportation, Homeland Security, and others "to enable civilian and commercial adoption of technologies and capabilities for resilient and survivable alternative positioning, navigation, and timing capabilities to complement the global positioning system" [2].

Because of the importance of PNT to all parts of DoD operations (movement, identification friend or foe, and targeting) and the increasing threat to the reliable use of GPS that the DoD is facing from different threat actors, all parts of the DoD are developing programs and research to address the need for APNT in different environments.

Sections 2.4.1 through 2.4.4 summarize some of these DoD APNT-focused programs. In addition to and in support of major programs within the Army, Air Force, Navy, the Defense Advanced Research Projects Agency (DARPA), and several allied nations, several of the major defense contractors have developed programs to support APNT requirements. Section 2.4.5 describes APNT-related projects being developed by major defense contractors.

2.4.1 U.S. Army

The U.S. Army has a robust set of programs related to PNT and APNT to support operations throughout Army and Joint operations and operations with allied forces. Figure 2 presents an overview of the U.S. Army's APNT program.

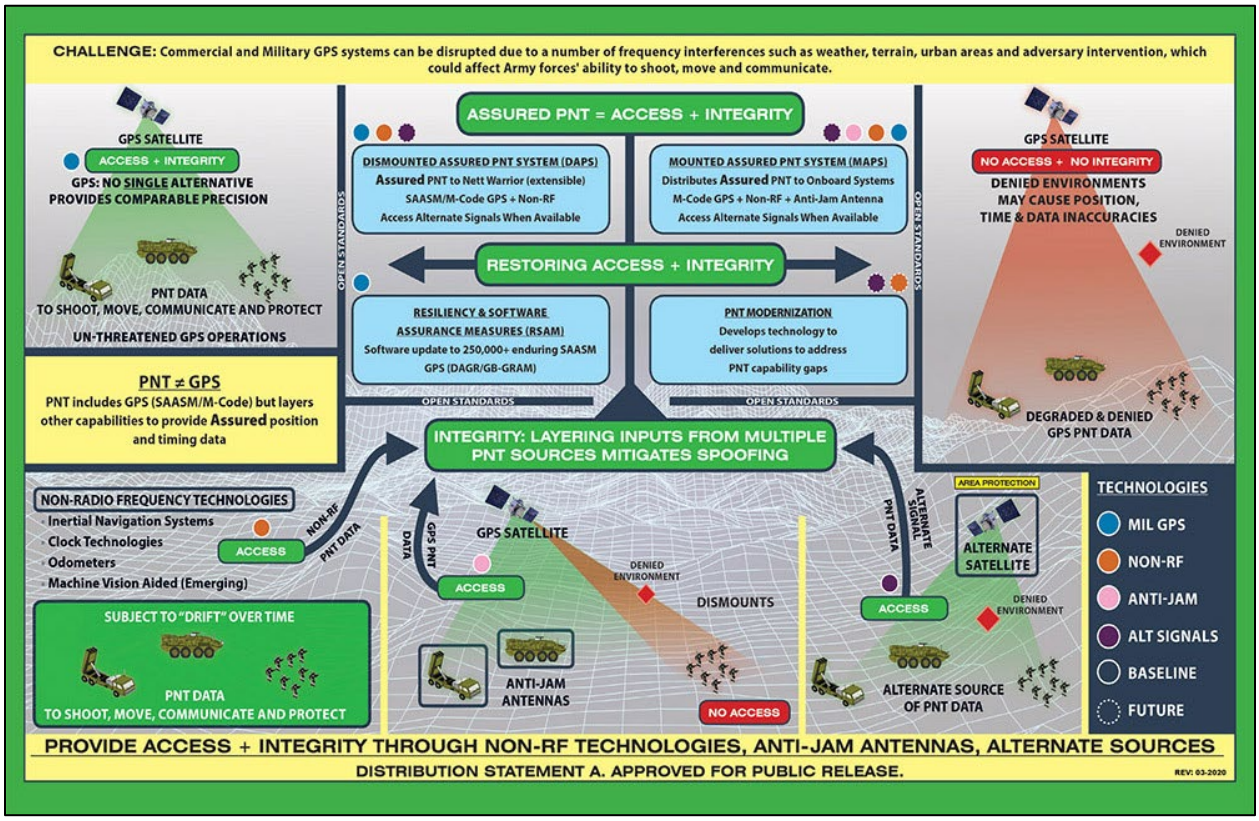

Figure 2: U.S. Army APNT Program [3].

Headquartered in Aberdeen Proving Ground, Maryland, Program Manager (PM) PNT is the Army's lead acquisition developer tasked with developing, modernizing, and integrating optimal and affordable PNT capabilities to promote decisive actions in Army operations. PM PNT reports to the Program Executive Office - Intelligence, Electronic Warfare & Sensors and collaborates with other Army and Joint Service partners to develop interoperable, reliable products to promote real-time, secure PNT services for a variety of combat and combat-support field missions. The acquisition and development of these capabilities will provide the soldier with access to accurate and trusted PNT data, which is critical for Army Warfighting functions and systems [3].

Mounted Assured PNT System (MAPS). The APNT Cross-Functional Team in Huntsville, AL, announced the approval of the MAPS Capability Development Document, which is the Army's first-ever PNT requirement. This document establishes an Army Program of Record to develop and field an enduring, advanced PNT capability to the Warfighter.

MAPS simplifies the Army's mounted PNT capability by distributing PNT data to multiple systems, eliminating the need for multiple GPS devices on a single platform. It will allow multiple users to access an assured GPS signal and other sources of PNT from one central point. This new PNT capability is paired with an antijam antenna system, allowing soldiers to operate in GPS-contested environments and giving them better antispoof and antijam capabilities [3].

2.4.2 U.S. Air Force

The Air Force and Space Force have the primary responsibility for both civilian and military GPS satellite systems.

Navigation Technology Satellite 3 (NTS-3). Contractor L3Harris Technologies announced on 5 February 2019 that an experimental Air Force navigation satellite had passed its preliminary design review, continuing a path to launch in 2022 [4]. NTS-3 is a major vanguard program being developed by the U.S. Air Force Research Laboratory (AFRL) and the Space and Missile Systems Center to demonstrate new PNT technologies that will inform how future GPS satellites work. L3Harris was awarded an $84 million contract through the Space Enterprise Consortium in 2018 to be the prime system integrator for NTS-3. The experimental satellite is on an aggressive development schedule, with plans to have it in orbit within 40 months from the time it was put under contract.

According to Arlen Biersgreen, Air Force NTS-3 PM [4],

> The NTS-3 vanguard is an experimental, end-to-end demonstration of agile, resilient space-based positioning, navigation, and timing. … It has the potential for game-changing advancements to the way the Air Force provides these critical capabilities to Warfighters across the Department of Defense. The commitment demonstrated by United States Space Force to partner with AFRL and support

technology transition was a key element in NTS-3 being designated as an Air Force vanguard in September 2019.

Due to how far in advance satellite acquisitions are planned out, the technologies on board NTS-3 likely will not be included on the current batch of 10 GPS III satellites, two of which are already in orbit. However, the technologies could inform the design and development of the GPS IIIF satellites, which will follow the fleet of GPS III satellites in the late 2020s. Lockheed Martin is the primary contractor for the Air Force on the GPS III program, and L3Harris provides the payload on those satellites.

Unlike other experimental satellites, NTS-3 could have an immediate benefit for the Warfighter. Once in geostationary orbit, NTS-3 will augment the GPS constellation. Because other GPS satellites are constantly moving in medium Earth orbit, NTS-3 will provide a unique, geographically focused PNT signal [4].

2.4.3 U.S. Navy

U.S. Naval Observatory (USNO) Master Clock (MC) [5]. The USNO in Washington, D.C. is responsible for maintaining precise time and making it available to DoD users. USNO's realization of UTC is the DoD standard and the primary time reference for GPS and other military applications. The precision of the USNO's MC makes it a popular reference choice for the Internet's Network Time Protocol (an Internet standard that facilitates the transfer of digital data). The MC is a major contributor to determining UTC, which is the primary international civil time reference.

The MC is an ensemble of dozens of independently operating atomic clocks, including cesium frequency standard clocks, hydrogen masers, and rubidium fountains. Its principal backup is the Alternate Master Clock Facility located at Shriever Air Force Base in Colorado Springs, CO. Most of the world's timing laboratories do not run continuously, but the DoD requires USNO to provide an uninterrupted time reference. No other continuously operating timing service maintains the precision of USNO's MC.

USNO's primary means for disseminating UTC is through GPS, on which more than 95 percent of military users rely for time transfer. USNO monitors the GPS constellation and provides system timing offsets and timing data for individual GPS satellites. There are two levels of GPS services [5]:

1. **Standard Positioning Service (SPS).** SPS is a positioning and timing capability available continuously to all [public] users worldwide, with no user fees. SPS uses the single-frequency GPS Coarse/Acquisition code in the L1 band, delivering predictable positioning accuracy of 9 m horizontally and 15 m vertically, and time transfer accuracy to within 40 ns of UTC.

2. **Precise Positioning Service (PPS).** PPS is a highly accurate positioning, velocity, and timing capability available to authorized military users. PPS uses the dual-frequency GPS P(Y) code in both the L1 and L2 bands, providing a more robust service than single-frequency SPS. It delivers positioning accuracy of 2.7 m horizontally and 4.9 m vertically and time transfer accuracy to better than 30 ns of UTC. PPS is denied to unauthorized users via encryption.

GPS-Based PNT Services (GPNTS). The Navy is currently modernizing its shipboard PNT fusion and distribution systems. The system under development is the GPNTS, which is designed to replace both Navigation Sensor System Interface suites and stand-alone military GPS receivers (WRN-6). GPNTS was scheduled for initial fielding in FY16 and will reach full operating capability in 2029. It will provide the fleet with more robust PNT in antiaccess/area-denial environments. Enhancements include the latest Selective Availability/Anti-Spoofing military GPS receivers; digital, nulling GPS antijam antennas; and redundant rubidium clocks for synchronized time and frequency. GPNTS is also the lead system for development and integration of maritime domain GPS receivers capable of receiving and using the new military-only M-code signal [5].

2.4.4 DARPA

DARPA has a robust, advanced PNT and APNT program of research to support the current and future PNT needs of the DoD. Figure 3 shows the key elements of DARPA's approach to PNT [6].

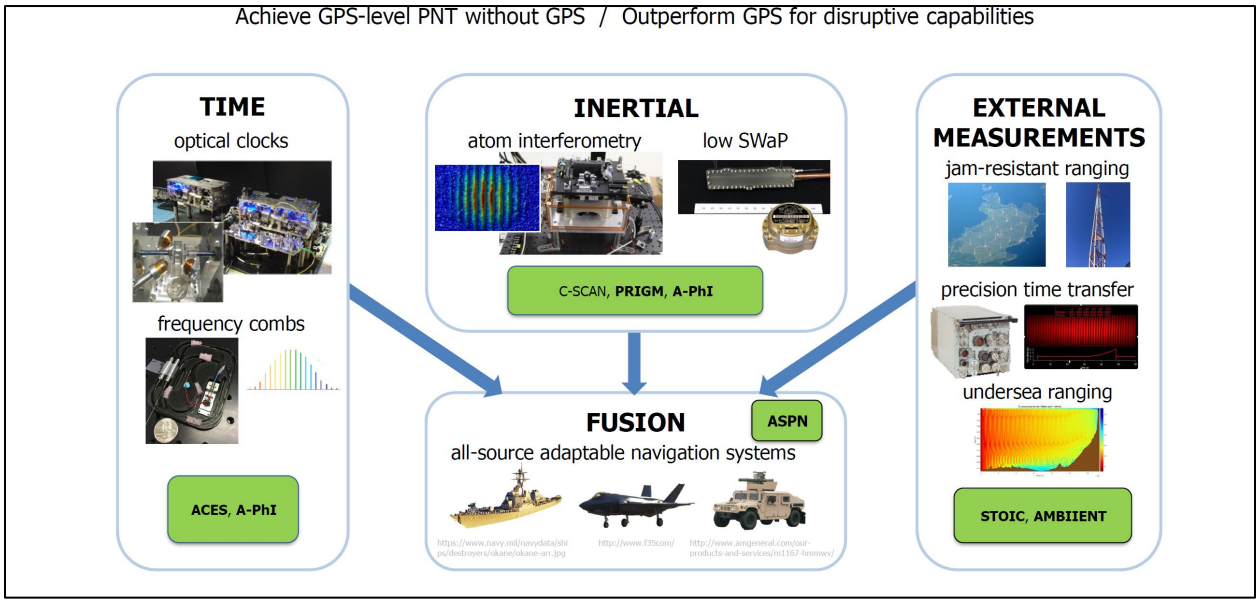

Figure 3: DARPA's PNT Approach [6].

2.4.5 Major Defense Contractors

To develop and field GPS, PNT, and APNT systems, the DoD uses a wide range of defense contractors. Major programs related to GPS, PNT, and APNT developed by Northrop Grumman, Raytheon, and Lockheed Martin are discussed in this section.

Northrop Grumman

Northrop Grumman's approach moves the burden of a trusted APNT hub away from sole reliance on GPS to the complementary use of inertial devices augmented with additional alternative methods of navigation. Figure 4 shows Northrop's approach to APNT.

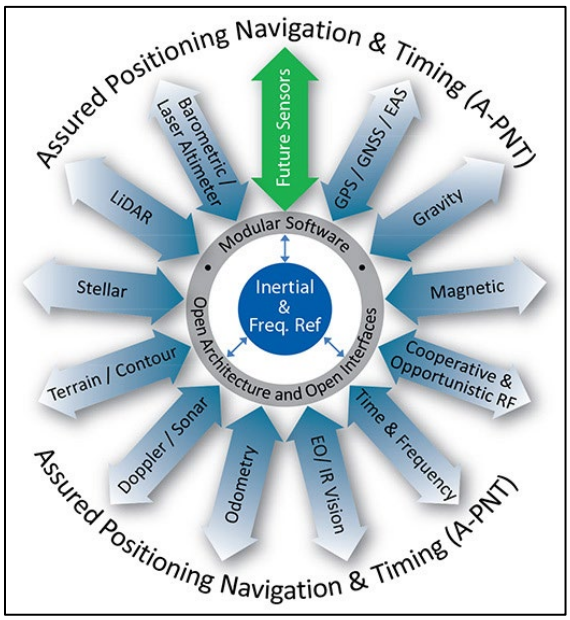

Figure 4: Northrop Grumman APNT Approach [7].

INSs calculate direction moved over time with a varying degree of drift, and with the use of high-precision oscillators, provide continuity of time. The great advantage of the INS is that it cannot be spoofed or jammed [7].

On an individual platform, there may be several sensors, each of which is a potential source of complementary information to support navigation. Northrop Grumman's solution harnesses as much of this sensor data as possible to contribute to an accurate and robust APNT solution, which will be trusted. The core of this philosophy is a software-defined open architecture that can affordably integrate data from diverse sensors, both GPS and non-GPS, in a single hub for distribution throughout the platform.

Raytheon

Raytheon was selected by the UK MoD Defence Equipment and Support office to develop a prototype system to exploit PNT information derived from GNSSs. Under the contract, Raytheon UK's APNT business will deliver a Technology Demonstrator Programme with advanced, multielement, antijam technology to prove the integration of this technology with a next-generation multi-GNSS receiver to both accelerate and reduce the risk of the availability of such systems to end users.

John Gallagher, Managing Director Weapons and Sensors, Raytheon UK, stated the following [8]:

> GNSS signals are used by many critical infrastructure organizations and the technology has transformed the way we live our everyday lives; however, the GNSS signals are susceptible to interference, both intentional and unintentional. The availability of low-cost jamming devices has meant that jamming is a constant threat.

Raytheon's antijamming technology will help mitigate the real, significant, and increasing threat of satellite signal interference and provide a future solution that will protect our front-line commands and critical National Infrastructure [8].

NavHub™-100 Navigation System

The Collins Aerospace (a Raytheon company) NavHub-100 is the navigational solution that generates and distributes APNT information to all systems onboard platforms through one device. The NavHub-100 key features are as follows [9]:

- Provides a high-assurance, accurate navigation solution across GPS threat environments with industry-leading Nav Fusion of multiple sensors.
- Implements modernized signal tracking to ensure GPS integrity.
- Supports Defense Advanced GPS Receiver standard interface.
- Includes an M-Code Security Certified Card.

Lockheed Martin

Lockheed Martin has fielded over 2,500 GPS Spatial Temporal Anti-Jam Receiver (GSTAR) systems and has now developed a modular, scalable family of solutions that can provide highly effective digital electronic protection for any platform that relies on GPS for navigation. They have designed, implemented, and tested a suite of reliable "building blocks" that can be quickly adapted to meet the specific needs of each platform as required. In addition, Lockheed Martin can field GSTAR antenna electronic units to any platform and for any contested condition, ensuring critical GPS operation.

Lockheed Martin describes GSTAR as a fully digital system that provides the strongest protection against adversarial jammers and spoofers; the high-end, beam-steering capability allows the host platform to survive the harshest of contested environments [10]. GSTAR can be configured as a nulling-only solution for compatibility with existing GPS receivers but can also be configured for beam-steering without replacement of the GSTAR or the antenna.

REFERENCES

[1] U.S. Department of Transportation. "What Is Positioning, Navigation and Timing (PNT)?" https://www.transportation.gov/pnt/what-positioning-navigation-and-timing-pnt, accessed 20 January 2021.

[2] Goward, D. "2021 Defense Act Signals Turning Point for Congress and PNT." https://rntfnd.org/2020/12/31/2021-defense-act-signals-turning-point-for-congress-and-pnt-gps-world/, 29 December 2020.

[3] PM PNT. https://pm-pnt.army.mil/home, accessed 20 January 2021.

[4] Strout, N. "A Milestone for the Air Force's Experimental Navigation Satellite." https://www.c4isrnet.com/battlefield-tech/space/2020/02/06/a-milestone-for-the-air-forces-experimental-navigation-satellite/, 6 February 2020.

[5] Deputy Chief of Naval Operations for Information Dominance. "Positioning, Navigation and Timing." https://www.doncio.navy.mil/CHIPS/ArticleDetails.aspx?ID=4618, 3 May 2013.

[6] Burke, J. "DARPA Positioning, Navigation, and Timing (PNT) Technology and Their Impacts on GPS Users." https://www.gps.gov/governance/advisory/meetings/2019-06/burke.pdf, 6 June 2019.

[7] Northrop Grumman. "Assured Positioning, Navigation, and Timing (PNT)." https://www.northropgrumman.com/what-we-do/air/assured-positioning-navigation-and-timing-pnt/, accessed 20 January 2021.

[8] Defense Mirror. "Raytheon to Develop Advanced GNSS Anti-Jamming Tech for UK." https://www.defensemirror.com/news/27478/Raytheon_to_Develop_Advanced_GNSS_Anti_Jamming_Tech_for_UK, 22 July 2020.

[9] Collins Aerospace. "Mounted Assured Positioning, Navigation and Timing System (MAPS) Gen II." https://www.collinsaerospace.com/what-we-do/Military-And-Defense/Navigation/Ground-Products/Mounted-Assured-Positioning-Navigation-Timing-System-MAPS-Gen-II, accessed 20 January 2021.

[10] Lockheed Martin. "GSTAR." https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/electronic-warfare/GSTAR%20Brochure.pdf, 2018.

BIOGRAPHY

Dr. Arndt is a leader in the development of technology and technology policy, with extensive experience as a senior executive and leader in the research, engineering, and defense industries. As an engineer, scientist, inventor, and engineering manager at several leading defense contractors, he was responsible for developing a wide range of communications, identifications, and counterterrorism technologies and systems. As Vice President and CTO of Ideal Innovations, he managed multimillion-dollar programs. He has served as a technical advisor for the Army, Defense Science Boards, National Science Foundation, IEEE, and International Standards Organization. He is a licensed Professional Engineer in the state of Ohio; published researcher in computer vision, artificial intelligence, biometrics, and counterterrorism; and holds six U.S. patents. Dr. Arndt holds a Ph.D. in electrical engineering from the University of Dayton; an M.A. in national security and strategic studies from the Navy War College; M.S.'s in human factors engineering and systems engineering from Wright State University; and a B.S. in electrical engineering from Ohio State University.