Global Positioning System (GPS) Selective Availability Anti-Spoofing Module (SAASM)

Executive Summary

- The Air Force upgraded the GPS Control Segment to the Architecture Evolution Plan (AEP) Version 5.5.4 and the Launch, Early Orbit, Anomaly Detection, and Disposal (LADO) system Version 5.8. They conducted a Force Development Evaluation (FDE) to support an operational acceptance decision in January 2012.
- The Air Force upgraded the GPS Control Segment to AEP Version 5.6 to provide Contingency Recovery and Over-the-Air Rekeying of military GPS receivers with Selective Availability/Anti-Spoof Module (SAASM).
- The Services conducted a Multi-Service Operational Test and Evaluation (MOT&E) to support a February 2012 decision for the Initial Operational Capability of the SAASM functions. Initial findings show SAASM to be operationally effective and suitable, but the Services need to place significant emphasis on ensuring that SAASM training/capabilities are utilized.
- SAASM is an enhanced GPS security architecture designed to provide over-the-air rekeying of GPS receivers in order to encrypt and decrypt the GPS signal. M-code will provide anti-jam capabilities.

System

- NAVSTAR GPS is an Air Force-managed, joint Service precision navigation and timing space program used for DoD and non-DoD operations.
- NAVSTAR GPS consists of three operational segments:
  - Space Segment - NAVSTAR GPS spacecraft constellation consists of a minimum of 24 operational satellites in semi-synchronous orbit.
  - Control Segment - The control segment consists of primary and backup GPS master control stations, operational system control antennas, a pre-launch compatibility station, and geographically dispersed operational monitoring stations.
    - AEP 5.6.2 is the current version of the control system supporting Blocks II/IIA, IIR/IIR-M, and IIF. AEP 5.7 will allow the command, control, and upload of different messages to sub-constellations of GPS satellites.
    - Next Generation GPS Operational Control Segment (OCX) replaces AEP and will support the current GPS constellation and the follow-on Block III satellites.
  - User Segment - There are many versions of NAVSTAR GPS mission receivers hosted on a multitude of operational systems and combat platforms.
- The system is being modernized with an M-code enhanced capability to better meet the needs of operational users. Future GPS updates will improve service in signal interference/jamming environments; enhance military and civil signal integrity; and provide time-critical constellation status.
- Air Force Space Command has launched four blocks of NAVSTAR GPS satellites and has one block of spacecraft in development:
  - Block I (1982-1992)
  - Block II/IIA (1990-1997)
  - Block IIR/IIR-M (Modernized) (1997 – 1999)
  - Block IIF development (May 2010 – present)
  - Block III development (replacement spacecraft)

Mission

- Combatant commanders, U.S. military forces, allied nations, and various civilian agencies use the NAVSTAR GPS system to provide highly accurate, real-time, all-weather, passive, common reference grid positional data, and time information to operational users worldwide.
- Commanders use NAVSTAR GPS to provide force enhancement for combat operations and military forces in the field on a daily basis throughout a wide variety of global strategic, operational, and tactical missions.

Major Contractors

- Block IIR/IIR-M/Block III: Lockheed Martin Space Systems – Valley Forge, Pennsylvania
- Block IIF: The Boeing Company, Integrated Defense Systems – Seal Beach, California
- OCX: Raytheon Company, Intelligence and Information Systems – Denver, Colorado

Activity

- The Air Force upgraded the Control Segment to support the Block IIF satellites and the 17th Test Squadron conducted an FDE in August and September 2010 for GPS AEP Version 5.5.4 and LADO system Version 5.8.
- The Air Force conducted a SAASM MOT&E in August 2011 with support from the Army Test and Evaluation Command; Commander, Operational Test and Evaluation Force; and the Marine Corps Operational Test and Evaluation Activity. This test will support the Initial Operational Capability decision by Air Force Space Command in February 2012. DOT&E will provide a report in 1QFY12.
- The Air Force conducted testing in accordance with the DOT&E-approved Test and Evaluation Master Plan (TEMP) and operational test plan.
- The next revision of the enterprise level TEMP is in coordination and expected for OSD approval in support of the OCX Milestone B scheduled for November 2011.

Assessment

- Initial SAASM MOT&E findings show it to be operationally effective and suitable but with some significant observations:
  - Emphasizing/enforcing the use of crypto-keyed GPS receivers will enhance operational utility in a jammed environment
  - Developing concepts of operations and techniques, tactics, and procedures for keying GPS receivers will allow Services to ensure operational effectiveness of each device
  - Information assurance during the SAASM MOT&E was limited to SAASM equipment only and did not incorporate the overall GPS enterprise
- Test planning to support fielding of military GPS user equipment on the proposed schedule will require a deeper understanding of OCX in order to design testing that is adequate to evaluate the operational effectiveness.

Recommendations

- Status of Previous Recommendations. The Air Force has addressed all but two previous recommendations.
  1. Planning should continue to focus on end to-end testing of OCX with GPS receivers (including ground equipment). Testing should ensure GPS receivers are capable of receiving and processing the new modernized signals and are hosted on representative platforms (i.e., ships, aircraft, land, and space vehicles) in operationally realistic environments.
  2. The synchronization of the development of the Space, Control, and User segments should continue to be monitored because delays in any segment will delay operational testing of all segments.
- FY11 Recommendations.
  1. The Air Force should ensure comprehensive and realistic information assurance testing is conducted of all external interfaces that support GPS operations and performance.
  2. The Services should emphasize/enforce the use of crypto-keyed GPS receivers.
  3. The Services should develop concepts of operations and techniques, tactics, and procedures for keying GPS receivers.