Spider Increment 1A M7E1 Network Command Munition

Executive Summary

- The Army uses Spider as a landmine alternative to satisfy the requirements outlined in the 2004 National Landmine Policy.
- Spider Increment 1A is an upgrade to the fielded Increment 1 system. The Increment 1A system has the requirement to fire anti-vehicular, obstacle-producing munitions and to operate seamlessly with mission command systems. The upgrade is backwards compatible with the Spider Increment 1 system and includes:
  - A new Remote Control Unit (RCU) with an enhanced colored map background
  - Updated software to promote ease of user operability
  - A Secure Mission Data Loader (SMDL)
  - An Interactive Electronic Training Manual (IETM)
- The Army conducted a Limited User Test (LUT) in 3QFY16. During the LUT, Spider Increment 1A demonstrated no new capability over the fielded system. Units accomplished their missions using Spider Increment 1A, but Increment 1A did not meet its reliability requirement and had cybersecurity vulnerabilities during the test.
  - Increment 1A demonstrated significant reliability problems during the LUT. The reliability threshold is 0.96 probability of having no failures during a 72-hour mission. During the LUT, the system computer achieved a 0.65 probability of completing a mission without a failure.
  - Increment 1A did produce anti-vehicular obstacles during the LUT. This capability existed with the fielded Increment 1 system, but was not previously demonstrated.
  - Increment 1A could not properly demonstrate the requirement to operate seamlessly with the classified mission command system. While it is technically possible for Increment 1A to exchange information in an unclassified environment using a surrogate mission command system, this is not operationally relevant since mission command systems must operate on a classified network. The Army is in the process of changing the seamless interoperability requirement from a threshold to an objective requirement. The Army has not yet approved the change.

System

- The Army uses Spider as a landmine alternative to satisfy the requirements outlined in the 2004 National Landmine Policy that directs the DOD to:
  - End use of persistent landmines after 2010
  - Incorporate self-destructing and self-deactivating technologies in alternatives to current persistent landmines
- The Army fielded Spider Increment 1 systems in FY09 under an Urgent Materiel Release. The system reached Initial Operational Capability in FY11 and obtained its Full Materiel Release in FY13.
- A Spider munition field includes:
  - Up to 63 Munition Control Units (MCUs), each housing up to 6 miniature grenade launchers or munition adapter modules (the modules provide remote electrical firing capabilities)
  - A remote control station, used by the operator to maintain "man-in-the-loop" control of all munitions in a field (this is the component upgraded in Increment 1A)
  - A communications relay device known as a Repeater for use in difficult terrain or at extended ranges
- Spider incorporates self-destructing and self-deactivating technologies to reduce residual risks to non combatants and has the capability to use non-lethal munitions such as the Modular Crowd Control Munition that fires rubber sting balls.

Mission

Brigade Combat Team commanders employ engineer units equipped with Spider to provide force protection and counter-mobility obstacles using lethal and non-lethal munitions. Spider functions as a stand-alone system or when combined with other obstacles to accomplish the following:

- Provide early warning
- Protect the force
- Delay and attrit enemy forces
- Shape the battlefield

Major Contractor

Command and Control hardware and software: Northrop Grumman Information Systems Sector, Defense Systems Division – Redondo Beach, California

Activity

- In January 2016, the Army conducted a Cooperative Vulnerability and Penetration Assessment. This assessment identified four cybersecurity vulnerabilities.
- In March 2016, the Army conducted a System Verification Test at Fort Leonard Wood, Missouri. Multiple Software Change Requests were submitted to the contractor based on this test.
- During May 2016, the Army conducted the Spider Increment 1A LUT at the Network Integration Evaluation 16.2 at Fort Bliss, Texas, in accordance with a DOT&E-approved Test and Evaluation Master Plan (TEMP) and test plan.
- During FY16, the Army continued its contract with Northrop Grumman to refine Spider Increment 1A software.
- At the end of FY16, the Army was updating the Spider Increment 1A TEMP to support a Milestone C decision and a projected IOT&E for FY18.

Assessment

- During the LUT, Spider Increment 1A demonstrated suitability and survivability deficiencies.
  - Operational effectiveness – A trained unit can employ Spider Increment 1A as a component of a protective obstacle and provide obstacle effects as intended by the commander.
  - Suitability – The system's computer did not demonstrate its reliability requirement during the LUT. The system is required to have a 0.96 probability of completing a 72-hour mission without failures. During the LUT, 13 of 20 missions had no essential function failures, resulting in the computer demonstrating a mission success rate of 0.65.
  - Survivability – Due to cybersecurity deficiencies, Spider Increment 1A components are not survivable in an operational environment.
- Based on the Capability Development Document, Spider Increment 1A demonstrated no new capability during the FY16 LUT.
  - Spider Increment 1A could not properly demonstrate the requirement to operate seamlessly with the classified mission command system. While it is technically possible for Increment 1A to exchange information in an unclassified environment using a surrogate mission command system, this is not operationally relevant since mission command systems must operate on a classified network.
  - A cross-domain solution that could enable two-way communication between unclassified and classified systems does not currently exist. The Army was aware of this cross-domain problem prior to the LUT and did not attempt to include this functionality during the test.
  - The Army is in the process of changing the Spider Increment 1A seamless interoperability requirement. The Program Office and user representatives propose downgrading the requirement from a threshold to an objective requirement. The Army has not yet approved the change.
- Increment 1A did produce anti-vehicular obstacles during the LUT. This capability existed with the fielded Increment 1 system, but was not previously demonstrated.
- The Army did not correct all identified cybersecurity vulnerabilities prior to the LUT. The Army plans on addressing and testing all cybersecurity deficiencies prior to the IOT&E.

Recommendations

- Status of Previous Recommendations. The Army corrected Spider Increment 1 deficiencies addressed in previous recommendations.
- FY16 Recommendations. The Army should:
  1. Design the Spider Increment 1A IOT&E to enable the characterization of the system's end-to-end mission effectiveness, over the maximum operational distance, to inform the system operators of its capabilities and limitations in the various conditions that will be encountered during combat operations. These conditions should include cyber and electronic warfare.
  2. Include doctrine, tactics, and techniques on engagement area development in unit pre-IOT&E training. The maneuver unit commander should assume the responsibility to ensure leaders, soldiers, and the Spider equipped engineer unit are trained properly. Training should include a situational training exercise on collective tasks related to engagement area development augmented by an engineer unit resourced with Spider Increment 1A systems.
  3. Resolve the problem between Spider Increment 1A and the mission command system preventing Spider Increment 1A from sending digital obstacle reports to the classified mission command systems. This will allow units to know in real time where Spider fields are located on the battlefield.
  4. Prior to IOT&E:
     - Develop, fund, and implement a comprehensive reliability growth plan to correct system reliability deficiencies.
     - Demonstrate fixes to the RCU, RCU Transceiver, MCU, and Repeater reliability and communication issues through testing.
     - Develop fixes for the known cybersecurity vulnerabilities.