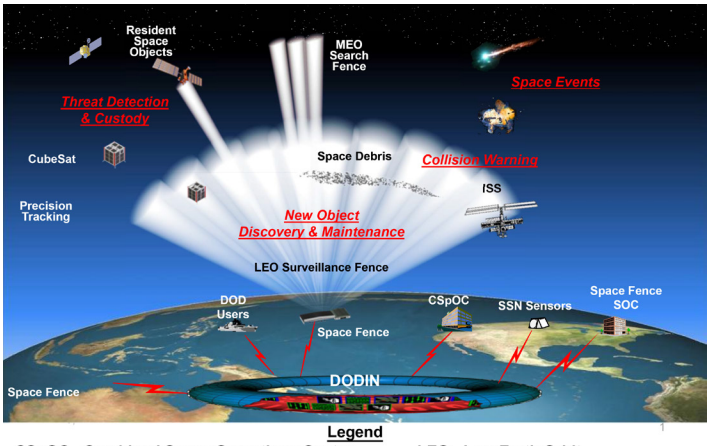
Space Fence (SF)

Executive Summary

- The Air Force Operational Test and Evaluation Center (AFOTEC) conducted an IOT&E of Space Fence (SF) Increment 1 from August 6 through November 1, 2019. Testing was adequate to determine SF operational effectiveness, suitability, and survivability when supporting the Space Force's Space Domain Awareness (SDA) mission.
- SF is operationally effective. Its observations improved the Space Force's SDA by cataloging previously untracked space objects and significantly increasing the total number of objects maintained in the satellite catalog.
- SF is operationally suitable. It maintained sufficient operational availability to support the SDA mission. However, operator workload was high because of system latencies on the operator network, requiring the use of the maintenance network as a workaround.
- SF is not survivable against insider or nearsider limited to moderate cyber threats. Testing discovered cybersecurity problems that could deny or degrade SF operations.

System

- SF is a space surveillance S-Band radar system integrated into the Space Surveillance Network (SSN). SF detects, tracks, identifies, and characterizes man-made Earth-orbiting objects in space.
- SF's primary capability is un-cued detection and tracking of objects (satellites, space debris, etc.) in low Earth orbit (LEO), with additional capability to detect and track objects in medium Earth orbit (MEO) and geostationary equatorial orbit (GEO).
- SF deployed Increment 1, which consists of a radar site at Kwajalein Atoll and an Operations Center co-located with the Reagan Test Site Operations Center in Huntsville, Alabama. Increment 2, a second radar site in Australia, is currently unfunded.



Mission

The 18th Space Control Squadron located at the Combined Space Operation Center uses SF to maintain a constant surveillance of man-made objects in space to support the SDA mission. SF provides high fidelity, un-cued, and cued radar observations from LEO, MEO, and GEO to the SSN. SF data supports the 18th Space Control Squadron satellite catalog maintenance and processing of space events (e.g., satellite maneuvers and breakup events).

Major Contractors

- Lockheed Martin Rotary and Mission Systems – Moorestown, New Jersey
- General Dynamics Mission Systems – Plano, Texas

Activity

- The Air Force conducted developmental test and evaluation (DT&E) from April to August 2019, in preparation for operational testing.
- AFOTEC conducted cybersecurity testing from January 28 to February 8, 2019; August 19 – 28, 2019; and September 9 – 19, 2019, to determine the cyber survivability of the system.
- AFOTEC and the Joint Navigational Warfare Center conducted GPS-resilience testing of the system in August 2019.
- AFOTEC conducted an IOT&E in accordance with the DOT&E-approved test plan from August 6 to November 1, 2019, with one exception: testing the radar in Flexible Coverage Mode was not completed in its entirety as planned.
- During DT&E and IOT&E, the Joint Interoperability Test Command (JITC) conducted an evaluation of the SF Net-Ready Key Performance Parameters.
- DOT&E also used data from the Air Force-conducted operational trial period in November through March 2020 to support the IOT&E report.
- The Space Force declared both initial operational capability and operational acceptance of SF on March 27, 2020.
- DOT&E published an SF IOT&E report in June 2020.

Assessment

- Testing was adequate to determine SF operational effectiveness, suitability, and survivability; however, competing test priorities limited the DOT&E assessment of the radar in Flexible Coverage Mode for space debris characterization.
- SF is operationally effective. SF improved the Space Force's SDA mission by increasing the frequency of tracking cataloged objects and by cataloging previously untracked space objects, significantly increasing the total number of objects maintained in the satellite catalog.
- Though the evaluation of SF in Flexible Coverage Mode was limited, the radar demonstrated the capability to track objects roughly the size of a cherry in LEO. With only one sensor site, SF does not have the power to continuously detect, track, and maintain awareness of all of these small objects.
- SF testing revealed two effectiveness concerns:
  - The system's parameters for operator-directed detection and tracking were not optimized for small, cube-shaped satellites, which are proliferating widely.
  - Switching between the primary and backup frequency and timing sources affects metric accuracy (some accuracies increase, while others decrease), but does not prevent SF from meeting accuracy requirements.
- SF is operationally suitable. It maintained sufficient operational availability to support the SDA mission. While SF was available to support mission needs, testing revealed three noteworthy suitability concerns:
  - Operators, system administrators, and system maintainers received insufficient training from Lockheed Martin to configure the system prior to testing.
  - High network latency caused status differences between operations and maintenance consoles, increasing operator workload.
  - System software instabilities caused the mean time between critical failures (MTBCF) to be two orders of magnitude worse than required, despite repeated attempts to resolve the concerns with software patches during IOT&E.
- SF operators are able to input taskings into the SF system. However, the system did not initially consistently plan, schedule, or conduct tasks correctly, leading to an increase in operator workload to monitor automatic taskings and missed observations. Software patches installed prior to regression testing largely addressed this problem, making the tasking process more streamlined for the user.
- Available system and user documentation lacked final corrections, processes, and procedures prior to operational testing. Incomplete documentation resulted in operators being unable to complete some tasks in a timely manner without subject matter expert involvement.
- SF is not survivable against insider or nearsider limited to moderate cyber threats. Testing discovered cybersecurity problems that could deny or degrade SF operations. Although some scenario-driven data collection was conducted, it did include an assessment of the local defenders' reactions to cyber threats. DOT&E will publish the cybersecurity findings, along with other threat-based testing results, in the classified annex of the SF IOT&E report.

Recommendations

1. The Space Force should modify operator-directed tracking to account for larger-than anticipated changes in radar cross section for cubic satellites, and retest the probability-of-detection requirement.
2. The SF Program Office should address the following:
   - Mitigate metric accuracy discrepancies between primary and backup frequency and timing sources, and retest to ensure that they produce commensurate results.
   - Characterize the Flexible Coverage Mode for its utility in supporting debris surveys.
   - Develop robust SF training programs for new operators, system administrators, and system maintainers.
   - Reduce the high network latency that caused differences between operations and maintenance consoles.
   - Continue to perform root-cause analyses of software failures, and implement system patches and fixes as necessary.
   - Mitigate all cybersecurity exposures and vulnerabilities identified during operational cyber testing before follow-on testing.
3. The Space Force should coordinate with AFOTEC and the SF Program Office to plan and conduct a follow-on cybersecurity adversarial assessment that focuses on the responses of the system defenders to adversarial activity and the verification of fixes to previously open cyber findings.