Next Generation Jammer Mid-Band (NGJ-MB)

The Navy Milestone Decision Authority approved the Next Generation Jammer Mid-Band (NGJ-MB) to proceed through Milestone C without completing the planned Capabilities Based Test and Evaluation period.

The Navy needs to overcome several challenges to demonstrate the NGJ-MB's operational effectiveness and suitability as it proceeds to IOT&E. The lack of validated or accredited digital models needed to supplement NGJ-MB operational flight testing present a significant risk to NGJ-MB IOT&E. The Navy and contractor continue to develop the system to resolve performance problems.

System Description

The NGJ-MB is an airborne electronic attack system. It consists of two pods mounted under the EA-18G aircraft wings that integrate with the AN/ALQ-218 radio frequency receiver. Each pod contains four active electronically scanned arrays, which radiate over a band of frequencies, and a ram-air turbine that generates internal power. The NGJ-MB is the first of the three NGJ programs intended to engage multiple advanced threats at greater stand-off ranges, compared to the legacy AN/ALQ-99 Tactical Jammer System.

Program

The NGJ is an Acquisition Category IC program being acquired in three separate acquisition programs: Increment 1 (Mid-Band (MB)), Increment 2 (Low-Band (LB)), and Increment 3 (High-Band (HB)). These will eventually replace all of the legacy ALQ-99 Tactical Jammer System pods that have been developed and fielded since 1971 on the recently-retired EA-6B Prowler and are currently flown on the EA-18G Growler. In May 2021, the Secretary of the Navy approved the NGJ-MB program to move past Milestone C, thereby authorizing procurement of low-rate initial production (LRIP) pods. The LRIP pods are scheduled for delivery beginning in September 2023. The first System Demonstration Test Asset (SDTA) shipset that supports IOT&E, scheduled for 2QFY23, will be delivered in February 2022. DOT&E approved the Milestone C NGJ-MB Test and Evaluation Master Plan (TEMP) in November 2020.

Major Contractors

- Raytheon Space and Airborne Systems – El Segundo, California.
- The Boeing Company, Integrated Defense Systems – St. Louis, Missouri.
- Northrop Grumman Mission Systems – Linthicum, Maryland.

Test Adequacy

No operational testing has been conducted on the NGJ-MB system thus far. For Milestone C, the Navy used a combination of ground-based testing, mostly in anechoic chambers, and early developmental flight testing to assess NGJ-MB performance against the system specifications. Since the Navy did not accomplish the planned early operational tests, they moved these tests to a Capabilities Based Test and Evaluation period just prior to IOT&E. If the tests are not accomplished prior to IOT&E, then they will occur during IOT&E and likely extend the planned IOT&E schedule.

The Navy is in the process of developing an incremental operational test strategy intended to provide the data required for an adequate verification and validation of critical modeling and simulation (M&S) needed to supplement NGJ-MB operational flight testing. This approach has been neither fully developed and vetted by the Navy nor approved by DOT&E.

In May 2017, the Navy conducted a Cyber Table Top event for the NGJ-MB, but has not yet completed a Cooperative Vulnerability Identification event identified in the DOT&E-approved TEMP.

Performance

Effectiveness

The Navy needs to overcome several challenges to demonstrate the NGJ-MB's operational effectiveness as it proceeds to IOT&E. As of Milestone C, the NGJ-MB system has achieved several key performance parameters, but is still underperforming in several important areas. The NGJ-MB design is not expected to undergo any major hardware changes, so additional system development will occur mostly through software updates. The Navy continues to test the system both in laboratories and in flight.

The lack of validated or accredited digital models needed to supplement NGJ-MB operational flight testing present a significant risk to NGJ-MB IOT&E. The Navy has a plan for validation, but has been unable to collect the data necessary to validate the models. The operational test team determined operational test flights would need to begin in 3QFY22 to collect the necessary data for model validation and to have the time to complete all planned operational test events by the planned end of IOT&E. The Program Office stated that the SDTA pods will likely be delivered to the operational test team later than 3QFY22, which may not allow sufficient time to validate, accredit, and use the digital models to supplement the flight test data. In addition, test data classification problems have prevented M&S personnel from analyzing the data.

Suitability

The Navy needs to overcome several challenges to demonstrate the NGJ-MB's operational suitability as it proceeds to IOT&E. Preliminary analysis is highlighted in the Controlled Unclassified Information edition of this report.

Survivability

No data are currently available to inform the NGJ-MB's survivability in a cyber-contested environment or take actions to address any identified vulnerabilities.

Recommendations

The Navy should:

1. Revise the NGJ-MB schedule as necessary to ensure sufficient time for completion of the ship-based testing, large-force exercises, tests against advanced radar signal emulators, and other important test events needed to support an adequate IOT&E.
2. Develop and codify its incremental operational flight test strategy and demonstrate that it can provide information to support adequate operational testing and provide the data necessary to validate the required M&S.
3. Obtain required security clearances for operational test and M&S personnel so they can access the test facilities and data needed to support the validation and accreditation of digital M&S tools required to evaluate operational effectiveness.

4. Complete the Cooperative Vulnerability Identification event required in the TEMP to identify vulnerabilities in the NGJ-MB system and allow the program to prioritize vulnerability resolution. This will facilitate more effective Cooperative Vulnerability and Penetration, and Adversarial Assessments during IOT&E.