

C-130J

Executive Summary

- The Air Force Operational Test and Evaluation Center (AFOTEC) completed IOT&E in March 2019 and published an IOT&E report in June 2019. DOT&E analysis of IOT&E data is ongoing.
- IOT&E data indicate that although the Block Upgrade 8.1 (BU8.1) modification provides the communications and navigation required to meet international airspace regulations, to continue performing the combat delivery mission, numerous shortfalls in usability, training, and technical data hinder the efficacy of the upgrade. The Air Force is planning subsequent software updates to address these shortfalls.
- AFOTEC conducted a cybersecurity Adversarial Assessment (AA) of a BU8.1 aircraft in March 2019 with some limitations caused by inadequate technical tools and lack of access to proprietary system software. Findings will be published in a DOT&E classified report in 2QFY20.

System

- The C-130J is a medium-sized, four-engine, turboprop, and tactical transport aircraft.
- The C-130J digital avionics and navigation systems enabled the Air Force to reduce the flight deck aircrew to two pilots, eliminating the navigator and flight engineer positions. Since fielding the C-130J, the Air Force has been implementing periodic Block Upgrades to improve workload and human factors for the reduced aircrew.
- BU8.1 provides navigation and communication updates to the C-130J to comply with International Civil Aviation Organization requirements and ensure continued access to civil airspace. It will field a Link 16 capability and deficiency corrections that were provided by the Block Upgrade 7.0, which the Air Force did not field after developmental testing.

Mission

- Combatant Commanders use the C-130J within a theater of operations for Combat Delivery missions that include:
 - Airdrop of paratroopers and cargo (palletized, containerized, bulk, and heavy equipment)

Activity

- AFOTEC conducted a cybersecurity AA of the C-130J BU8.1 as the final IOT&E test event at Little Rock AFB, Arkansas, in March 2019. The 57th Information Aggressor Squadron portrayed the cyber threat.
- AFOTEC conducted the cybersecurity AA test in accordance with the DOT&E-approved AA plan, but some deviations from the plan were necessary during execution due to



Air Force Operational Test and Evaluation Center Operational Test Director observing Block Upgrade 8.1 operational testing.

- Air-land delivery of passengers, troops, and cargo
- Emergency aeromedical evacuations
- Combat Delivery units operate globally in civil-controlled airspace and in all weather and lighting conditions.

Major Contractor

Lockheed Martin Aeronautics Corporation – Fort Worth, Texas

inadequate technical tools and the lack of access to proprietary system software.

- AFOTEC published an IOT&E report in June 2019 and a classified cybersecurity annex in August 2019.
- The Air Force approved the Full-Rate Production decision on the BU8.1 retrofit in October 2019.

FY19 AIR FORCE PROGRAMS

- AFOTEC conducted testing consistent with the C-130J Block 8.1 Test and Evaluation Master Plan, approved by DOT&E on March 15, 2018.

Assessment

- DOT&E analysis of IOT&E data was ongoing at the beginning of FY20.
- The C-130J BU8.1 remains capable of performing the air-land and airdrop combat delivery missions with improved navigation capabilities, but key components of the BU8.1 upgrade increased aircrew workload or fell short of operational requirements.
- Overall system reliability enabled maintenance personnel to support the necessary sortie generation rate during IOT&E in spite of shortfalls in integrated diagnostics, technical data, and training.
- Key BU8.1 communication and navigation upgrades enable C-130J compliance with Global Air Traffic Management requirements and continued access to worldwide airspace. Those subsystems include Automatic Dependent Surveillance-Broadcast Out; civil datalinks; and Required Area Navigation (RNAV)-compliant dual flight management system.
- Failures of the Communication/Navigation/Identification – System Processors (CNI-SP), observed on 11 of 52 missions, increased aircrew workload and led to 5 mission failures. Persistent failure of CNI-SP will jeopardize access to portions of RNAV-regulated airspace.
- The Link 16 upgrade does not support enhanced C-130J interoperability. A draft C-130J Link 16 concept of operations (CONOPS) was utilized during Block 8.1 IOT&E. The lack of implementation of a Link 16 CONOPS in Air Mobility Command (AMC) hinders successful connection to tactical networks. AMC is in the process of developing a Mobility Air Forces Link 16 CONOPS. Hardware and software

usability shortfalls hinder aircrew operation of the system. The Program Office is working with the Air Force System Interoperability Test organization and the Joint Interoperability Test Command (JITC) towards interoperability certification.

- Shortfalls in controls and displays, civil datalinks, and voice communications contributed to increased aircrew workload, decreased system usability, or decreased aircrew situational awareness.
- The cybersecurity AA was limited by lack of access to contractor proprietary information and incomplete technical tools on the part of the cyber-threat operators team (such as datalink test tools). The AA was sufficient to demonstrate mission-limiting shortfalls. Further results will be published in a classified report.
- BU8.1 is the last block upgrade for C-130J; the Air Force intends to continue deficiency corrections and capability enhancements through primarily software-based capability management upgrades (CMU). CMU 1 was already in development prior to BU8.1 IOT&E and is unlikely to address any deficiencies identified in that test. Deficiency reports issued by AFOTEC and an interim status report of the IOT&E informed planning for CMU 1C, which is intended to fix the most critical problems, notably the CNI-SP failures. The Air Force intends to field CMU 1C in FY21. Other problem areas will be addressed in CMU 2 planned for fielding in FY24.

Recommendations

The Air Force should:

1. Address CNI-SP failures and other Deficiency Reports, and verify corrections in follow-on testing.
2. Fully implement the Link 16 CONOPS and demonstrate interoperability in follow-on testing with JITC.
3. Develop or identify advanced cybersecurity test tools and conduct cybersecurity testing during FOT&E in areas that the IOT&E AA did not address.