# Battle Control System – Fixed (BCS-F)

**Executive Summary**

- The Air Force completed FOT&E on the Battle Control System – Fixed (BCS-F) Increment 3, Release 3.2.2 (R3.2.2) at all U.S. air defense sites in April 2014.
  - The BCS-F R3.2.2 is operationally effective with workarounds and operationally suitable, with deficiencies in documentation and training.
  - BCS-F R3.2.2 is still not survivable against potential cyber attacks despite the Air Force's efforts to improve R3.2.2's critical cybersecurity deficiencies.
- All U.S. air defense sites were utilizing R3.2.2 in February 2014. Upon completion of the FOT&E, the Air Force formally fielded R3.2.2.

**System**

- BCS-F is the tactical air battle management command and control system for the two continental U.S. North American Aerospace Defense Command (NORAD) air defense sectors, as well as the Hawaii and Alaska Regional Air Operations Centers. The system utilizes commercial off-the-shelf hardware within an open-architecture software configuration, and operates within the NORAD and U.S. Pacific Command air defense architecture. The system is employed by the U.S. and Canada.
- The R3.2 upgrade includes the following system enhancements:
  - Improved tactical datalinks with additional Link 16 and Link 11 message types that enable the operators to better digitally control fighters, send amplifying intelligence information, and create a more comprehensive air picture
  - Air Tasking Order and Airspace Control Order integration with Theater Battle Management Core Systems data sources that enables the operators to view the most current Air Tasking Order/Airspace Control Order and correlate the information with military aircraft
  - Data modification tools that enable system administrators to field changes to system files and to perform error checks with greater fidelity than R3.1
  - System control manager interface improvements that enable the system administrator to use improved system performance monitoring and diagnostics
  - Global Area Reference System coordinate conversion tool that facilitates a NORAD interface with global search and rescue efforts by using a common set of coordinates
  - Remote Gateway Manager control through the virtual network computing interface that provides the operators a complete picture of the available datalinks and flexibility to access link information from an operator workstation
  - Auxiliary server for offline training and support capabilities at the U.S. air defense sectors

  - Improved system capacities from 10,300 to 15,000 system tracks to support single sector, continental U.S. operations
- The R3.2.2 upgrade includes the following enhancements:
  - Ability to operate with mandatory International Civil Aviation Organization flight plan changes
  - Addition of external firewall/intrusion detection system sensor
  - Implementation of remote administrative management and log server capabilities
  - Audible and visual alert capabilities on the Computer Network Defense components
  - New network switch to support the Information Assurance-Demilitarized Zone architecture
  - Newly-designed protocol converter replacing the NORAD forward tell serial communications device. (This change replaces obsolete equipment and ensures the air picture from the sector will continue to be received at NORAD.)

**Mission**

- NORAD and U.S. Pacific Command Commanders use BCS-F to execute command and control and air battle management in support of air sovereignty and air defense missions for North American Homeland Defense and Pacific Command air defense.
- Air defense operators employ BCS-F to conduct surveillance, identification, and control of U.S. sovereign airspace and control air defense assets, including fighters, to intercept and identify potential air threats to U.S. airspace.

**Major Contractor**

Thales-Raytheon Systems – Fullerton, California

**Activity**

- The Air Force completed FOT&E on R3.2.2 at all U.S. air defense sites from September 2013 to April 2014. The Air Force Operational Test and Evaluation Center (AFOTEC) produced an FOT&E report on July 18, 2014.
- All U.S. air defense sites were utilizing R3.2.2 in February 2014. Canadian air defense forces were utilizing R3.2.2 in May 2014. Upon completion of the FOT&E, the Air Force formally fielded R3.2.2.
- AFOTEC and Air Combat Command conducted operational testing in accordance with a DOT&E-approved Test and Evaluation Master Plan and test plan.
- On August 13, 2014, DOT&E published a Major Automated Information System FOT&E report on BCS-F R3.2.2

**Assessment**

- R3.2.2 resolved two of the five major operational effectiveness deficiencies associated with battle management discovered during R3.2 and R3.2.0.1 operational testing. Additionally, FOT&E of R3.2.2 revealed four new deficiencies associated with battle management operations. Operator workarounds mitigated these deficiencies to an acceptable level.
- R3.2.2 is operationally suitable, although the Air Force did not collect sufficient operational test data to demonstrate the availability and reliability requirements with statistical confidence.
  - During 952.35 hours of testing, R3.2.2 did not experience any critical failures or downtime. One critical failure occurred after system fielding resulting in two hours of system downtime. Including this failure in total system operating time during the FOT&E resulted in an operational availability of 99.99 percent (80 percent confidence intervals are 99.78 and 99.99 percent).
  - Additionally, as of September 30, 2014, the system has operated at all four U.S. air defense sector sites without any additional critical failures since February 2014. This equates to over 23,000 hours (5,800 hours at each of four sites) with only one critical failure. The system requirement for Mean Time Between Critical Failure (MTBCF) is greater than or equal to 10,000 hours. Current data indicate with a 66.9 percent confidence that the MTBCF requirement has been met.
- R3.2.2 was maintainable for routine maintenance actions, but the observed 8.6 hour Mean Time Between Corrective Maintenance Action (MTBCMA) did not meet the 100-hour requirement. This was not a critical shortfall since the maintenance actions had no negative effect on operations or operator workload.
- While R3.2.2 is operationally suitable, technical documentation and training for the system administrators was deficient.
- R3.2.2 remains deficient in all cybersecurity assessment areas. The system is poorly equipped to detect, protect, react, and restore/recover from attacks by current cyber threats despite the fact that R3.2.2 was designed to resolve many critical cybersecurity deficiencies. The Air Force plans to address some of the outstanding cybersecurity deficiencies through implementation of the Computer Network Defense Service Provider agreement in 1QFY15.

**Recommendations**

- Status of Previous Recommendations. The Air Force satisfactorily addressed all but three of the previous recommendations. The Air Force still needs to:
  1. Correct and formalize all BCS-F Increment 3 system documentation and training deficiencies.
  2. Develop a plan for remote workstation management to include sustainment, training, documentation, and Information Assurance compliance.
  3. Upgrade the System Support Facility to support a more robust BCS-F developmental and operational testing capability in order to minimize the impact of overall testing at the operational sites.
- FY14 Recommendations. The Air Force should:
  1. Correct the three remaining operational effectiveness deficiencies discovered during R3.2 and R3.2.0.1 testing, as well as the four new deficiencies associated with battle management discovered during R3.2.2.
  2. Correct and formalize all BCS-F R3.2.2 documentation and training deficiencies.
  3. Improve reliability to meet the threshold requirement for MTBCMA.
  4. Fully assess system vulnerabilities and correct identified cyber deficiencies.
  5. Re-evaluate BCS-F survivability against cyber attacks after the Computer Network Defense Service Provider has been implemented. This evaluation is scheduled to occur in 1QFY15.
  6. Implement appropriate policies, procedures, and tools for system administrators to effectively respond to unauthorized intrusions.
  7. Correct network configuration deficiencies to more effectively detect unauthorized intrusions.