CASE STUDY

Airplane Developer Looks to Protect ISR Data with Encryption

CURTISS-WRIGHT

DEFENSE SOLUTIONS

Challenge

- Needed Ethernet-based computer, sensors, and data concentrator
- Centralized, encrypted data storage required
- Data off-load ground station critical for the program

Solution

- DTS3 network attached storage device with AES256
- Three 2 TB removable memory cartridges
- SATA-to-USB device connecting to ground station

Results

- All devices share data seamlessly
- Massive storage with encryption protected data
- Convenient high-speed data upload and offload

Challenge

While developing a new intelligence, surveillance, and reconnaissance (ISR) system, a large aerospace developer approached Curtiss-Wright for commercial off-the-shelf (COTS) equipment that had to fit into a space-constrained, propeller-driven aircraft. For all the ISR equipment to communicate seamlessly, the new system required an Ethernet-based solution. The mission computer, sensors, and data concentrator would communicate via Gigabit Ethernet (GbE) with a switch in the middle. The plan was to share the data between network clients using a network attached storage (NAS) device. Since maps and mission plans would be transferred from a ground planning station to the new aircraft, the NAS had to include removable storage with multiple terabytes of capacity. With sensitive data being transported, the data had to be protected with powerful encryption. Data collected during the mission from sensors and other devices would also be transported back to the ground station for post-mission analysis. And, since propeller-driven aircraft have high shock and vibration levels, the NAS device had to be rugged.

The plane might loiter in the air for long periods of time collecting tremendous amounts of mission data. Because of the vast amount of data being collected, the integrator required a solution with massive storage, 4 TB storage capacity or more. AES256 bit encryption was preferred to protect the sensitive data being transported back and forth.

The integrator also needed a ground station device that the removable memory could be connected to, decrypted, and downloaded on a computer via USB.

DTS3 3-slot rugged network attached file server

Solution

After considering the program requirements, the system integrator selected the Curtiss-Wright DTS3 for their data storage solution. The DTS3 is equipped with four GbE data ports and supports industry standard protocols, including Network File System (NFS), Common Internet File System (CIFS), file transfer protocol (FTP), iSCSI, and HTTP. The DTS3 also supports PXE boot, a form of netbooting that enables network clients to boot directly from the DTS3 instead of requiring local storage in each individual network client. Using PXE boot, the customer can centrally manage and update multiple network clients from a single location. To meet the program's encryption requirements, the DTS3 protects data with a FIPS-certified, AES256-bit encryptor.

The DTS3 houses three removable memory cartridges (RMC) with storage from 256 GB to 2 TB for each RMC. The customer chose to use three 2 TB RMCs. The RMC has also been designed to reliably support programs for many years with a 100,000-insertion cycle connector that hosts a SATA interface. When the RMC is unplugged and unpowered during transport between the aircraft and the ground station, the RMC and the encrypted (Black) data on it are considered unclassified. The RMC download station was selected to offload post-mission data from the RMC and allow the mission planning computer to access the data. This small device decrypts the Black data and converts SATA from the RMC to USB for the ground station computer. The USB port can be virtually connected to any computer to off-load data from the RMC.

Results

The selection of the DTS3 allowed the customer to seamlessly integrate the rugged NAS device with other devices, such as their mission computer, for data recording and storage. The system's GbE capabilities made the transfer of the high-speed data possible.

With 6 TB total storage capacity exceeding the requirements, the integrator was able to capture vast amounts of data on the long-range missions of the propeller plane. The sensitive data is first encrypted with AES256-bit encryption prior to storage, ensuring the data is properly protected.

The customer was able to store their data on the RMC, remove it, and transport it to the ground station. With the simple SATA-to-USB (with encryption) converter, the mission planning system could load plans and maps onto the RMC prior to the mission and could off-load the captured sensor data after the mission.