Military
EMBEDDED SYSTEMS

Data-At-Rest recorder from Macrolink, now includes NSA Type 1 certified encryptor for unattended operation

 John McHale Editorial Director
Share on linkedinLinkedInShare on twitterTwitterShare on rssRSSShare on email

Engineers at Macrolink, a BE Aerospace Company, achieved National Security Agency (NSA) embedment approval for the company's Data-At-Rest (DAR) Recorder targeted for unattended operation on unmanned platforms. This is a big win for Macrolink and as far as I know it is the first solution of its kind available to the industry. It also builds on a discussion in our February/March issue of Military Embedded Systems magazine.

The availability of this type of system was covered that issue in an article titled "'Keys' to COTS encrypting of data-at-rest," by Paul Davis, Director of Product Management at Curtiss-Wright Defense Solutions. The article suggested that this new product may be more timely to industries' needs than was previously thought. In the article Davis writes:

"For applications that require TSABI security, an encryption product will need a minimum of NSA Type 1 certification. A few TSABI encryptors, developed at government expense for a program of record, are currently available for DAR applications. At present, none of these encryptors have been certified for unattended operation on platforms such as unmanned air, ground, or undersea vehicles. Currently, some programs are considering combined requirements for TSABI and unattended operation. It will require one program of record and a Department of Defense (DoD) sponsor to step forward and drive TSABI encryptor certification for unattended operation."

This process is moving faster than previously thought as Macrolink's announcement and NSA certification story shows. The following is an exclusive to Military Embedded Systems.

"Government and Military data storage and recording applications must address the expanding need for strong encryption to protect sensitive data," says Jim Grace, Director of Business Development at Macrolink. "Deployed systems are now dominated by rugged solid state drives (SSDs) that have replaced spinning media. Sensitive data can be minimally protected with encryption built into SSDs. Applications demanding stronger encryption schemes need to be encrypted based on the sensitivity of data to be protected by the FIPS-140-2 standards, while more sensitive data needs to be protected to the IASRD Type I standard, which can protect data at levels to Top Secret.

“It is a well known fact that only NSA Type I certification provides the approval for DAR systems that demand protection for Secret And Below (SAB) or Top Secret And Below (TSAB) data classifications,” Grace says. “It should also be further noted that complications arise in applications involving unmanned platforms [in the air, at sea, or on the ground]. For these unique deployments, the DAR system needs to be embedment approved by the NSA for unattended operation. To achieve this approval level the platform also needs to be reviewed and approved by the NSA to insure a properly secured feed to storage subsystem.

"The certification process for a system of this type can be quite long and requires a ‘program-of-record’ sponsor,” Grace continues. “As stated in the referenced article, and until this year, such a system has been unavailable. Now Macrolink would like to correct the perception that this capability is not available to industry, as Macrolink has completed development and a program of record has deployed, at Low Rate Initial Production (LRIP), a product for the unattended operational need. This product, packaged within a ¾ ATR enclosure, meets full military requirements for flight certification and features as much as 10 TB or more of SSD storage (subject to capacity of available drives).”

Macrolink’s TSAB system is available today for adaption into applications performing in unattended environments, according to Grace. The stored, encrypted DAR on the removable flash storage array (FSA) is trusted and essentially unclassified. The removable FSA can be quickly replaced, reducing mission downtime. Macrolink provides ground stations that enable the removed FSA data to be downloaded and/or decrypted as required. The deployed system also features a Cryptographic Ignition Key (CIK) qualified for use on government-sponsored platforms.

For more information on the Macrolink solution, contact Jim Grace at 714 777-8800 (Ex307).