

Rad-T Reprogrammable Cryptographic Solution

Radiation Tolerant ASM Programmable Cryptographic Module

Key Features

Rad-Tolerant Version of ASM

- Functional TMR'd FPGAs
- High Assurance Checking Logic
- FPGA Configuration Authentication
- FPGA Configuration Scrubbing
- Memory EDAC and Scrubbing
- Rad-Hard NV Memory
- Supports 1 to 4 Traffic Channels
- High Speed Traffic Channels
 - 1.25 Gbps per channel Tx & Rx
 - SERDES Interface
- Four 4 low speed serial Interfaces
 - 0 to 200Mhz Interface
 - Supports Legacy Interfaces

Encryption/Decryption Modes:

- Suite A Algorithms
- Suite B Algorithms
- Legacy Algorithms
- BIP-32, SHA-1, SHA-384 Data Integrity
- Multiple Single Levels of Security (MSLS)
- Multiple Simultaneous Independent Crypto Channels

Key Management:

- DS-101
- DS-100 Key Tagging
- Key Wrapping/Unwrapping and Updating
- Key Storage (1000+)
- Firefly Versions 9.1 and 17.1
- Enhanced Firefly
- Multiple Universal Key Sets (10+)

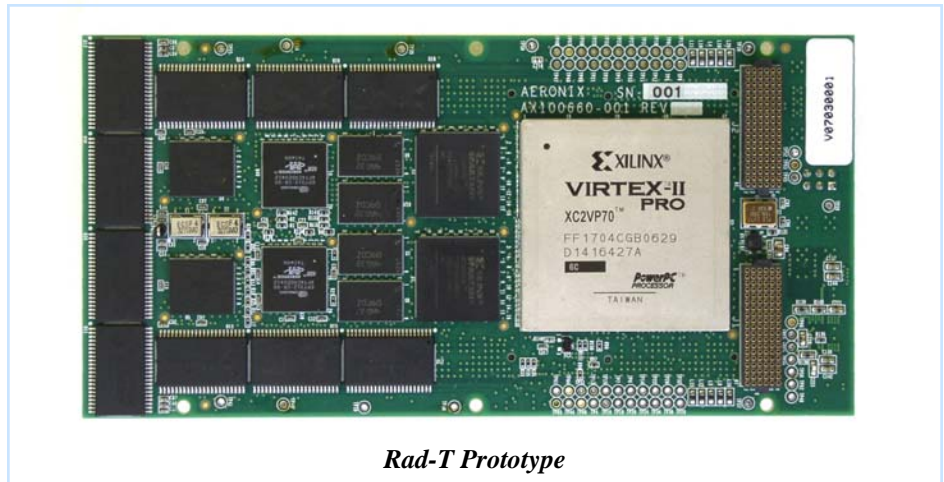
Additional Security Functions:

- Unclassified Prior to Programming
- CCI After Activation
- Access Control Lists
- High Speed Randomizer
- Programmable Cryptographic Bypass
- Secure Authentication for Remote Management
- JOSEKI Decrypt
- Signature Verified Software Download
- Signature Verified Algorithm Download
- Embedding Equipment Unique Access Control, Bypass, and Audit Security Policies

The Rad-T ASM is an SBIR Phase II development with AFRL, Kirkland. Aeronix will deliver four working Rad-T ASM prototypes in April 2007.

This Rad-T ASM is a radiation tolerant version of the terrestrial ASM module. The Rad-T ASM supports the requirement sets of the Crypto Modernization Initiative, HAIPIS encryptor equipment, and the Joint Tactical Radio System (JTRS). Rad-T ASM products are suitable for embedment in a wide range of End Crypto Units (ECUs) and address additional requirements necessary for operation in radiation harsh environments.

ASM's innovative architecture permits straightforward evaluation and simplifies incorporation of design variants. Maximum use of COTS technology and components mitigates technology obsolescence risks. ASM supports 100% field re-programmability for all firmware, software, key management, and crypto control algorithms. One-time programmable capability is also supported.



Rad-T Prototype

ASM Features	
Certification	Certifiable Design. Aeronix is actively seeking a Program of Record.
Classification	Unclassified Prior to Module Activation, CCI After Activation
Cryptography	Reprogrammable - Suite A/B and Legacy Algorithms
Data Classification	System High Up To Top Secret, Multi-Channel MSLS Up To Secret
Data Channels/Rate	1-4 Full Duplex Channels TTL DC to 100+ Mbps/Channel (800 Mbps Aggregate Data Rate) or CML/LVDS 1.25 Gbps/Channel (10 Gbps Aggregate Data Rate)
Bypass Channel(s)	Common Bypass and/or Channel/Algorithm/Waveform Specific Bypass
Key Management	Benign Key/Fill, Firefly, Enhanced Firefly, and OTAR
Security Policies	Embedding Equipment Unique Bypass, Access Control, and Audit Policies
100% Reprogrammable	All Firmware, Software, and Crypto Algorithms
Size	Multiple Form Factors as Small as 3" x 3" x 0.75"
Low Power	Less than 3.5 Watts at 100 Mbps



1775 West Hibiscus Boulevard ■ Suite 200 ■ Melbourne Florida 32901 ■ Tel.(321) 984-1671 ■ Fax.(321) 984-0366

www.aeronix.com