U-RTK Gryphon AES ASIC
NSA-Certified Fully Integrated Satellite Link Security Solution

Specifications

- **Uplink Algorithm:**
  - AES-256 (NIST FIPS-197) Modes: ECB, CTR, GCM, and CFB
  - Authenticated Command Modes: GCM and ECB with VCC (Vehicle Command Count)
- **Downlink Encryptor Algorithm:**
  - Fail-Safe Redundant AES-256 Modes: CTR, GCM, and CFB
  - Random number generator (RNG) for initial vector generation
- **Over-the-Air Rekey (OTAR):**
  - AES-256 ECB per NIST AES Key Wrap Spec
  - In-band or in-flight transferring of black key
- **Interfaces:**
  - Traffic, Key PROM, Command, and Control
- **Uplink Traffic Interface:**
  - Serial LV/TTL clock, data, and enable
- **Downlink Traffic Interface:**
  - Serial LV/TTL clock and data
  - 8/16-bit parallel clock and data

This Type 1 640 Mbps features low-power and is Radiation Hardened.

Features available for the first time in a space crypto solution:

- Multiple cryptographic modes and flexible synchronization logic support many mission profiles and CONOPS
- GCM cryptographic mode supports variable length authenticated commands up to 4k bytes in length.
- Authenticated downlink capability is ideal for tactical applications, such as UHF radios
- Multiple authenticated command channels enable direct payload or satellite tasking from tactical and/or multiple users
- Highly integrated single chip solution for both command uplink and data downlink security reduces footprint

- Unclassified design for high risk-of-loss environments and coalition partners

Additional Advantages:

- Protects data traffic up through TS/SCI
- Interoperable with KIV-7M Enhanced Suite B Gryphon GOE
- Radiation hardened 1 MRad (Si), latch-up immune, QML-V
- Unclassified and CCI when not keyed
- Over-the-Air Rekey (OTAR) capability to extend mission service life and allow dynamic crypto net management
- Radiation hardened to support all orbits
- On-chip synchronization detection reduces need for external circuitry
### Additional Specifications

<table>
<thead>
<tr>
<th><strong>Key PROM Interface:</strong></th>
<th>Adresses up to 512 keys</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Data Rates:</strong></td>
<td></td>
</tr>
<tr>
<td>Uplink</td>
<td>100 bps to 40 Mbps</td>
</tr>
<tr>
<td>Downlink</td>
<td>100 bps to 40 Mbps (serial), 320 Mbps (8-bit parallel) and 640 Mbps (16-bit parallel)</td>
</tr>
<tr>
<td><strong>Operating Temperature:</strong></td>
<td>-55 to +125°C</td>
</tr>
<tr>
<td><strong>Package Size:</strong></td>
<td>208-pin CQFP, 29.1 x 29.1 mm²</td>
</tr>
<tr>
<td><strong>Power:</strong></td>
<td></td>
</tr>
<tr>
<td>Supply Voltage</td>
<td>+3.3VDC</td>
</tr>
<tr>
<td>0.2W @ 1Mbps; 0.6W @ 20 Mbps; 2.8W @ 640Mbps</td>
<td></td>
</tr>
<tr>
<td><strong>Technology:</strong></td>
<td>0.35 micron, SOI, 1MRad</td>
</tr>
<tr>
<td><strong>MTBF:</strong></td>
<td>~1,000,000 hours</td>
</tr>
</tbody>
</table>