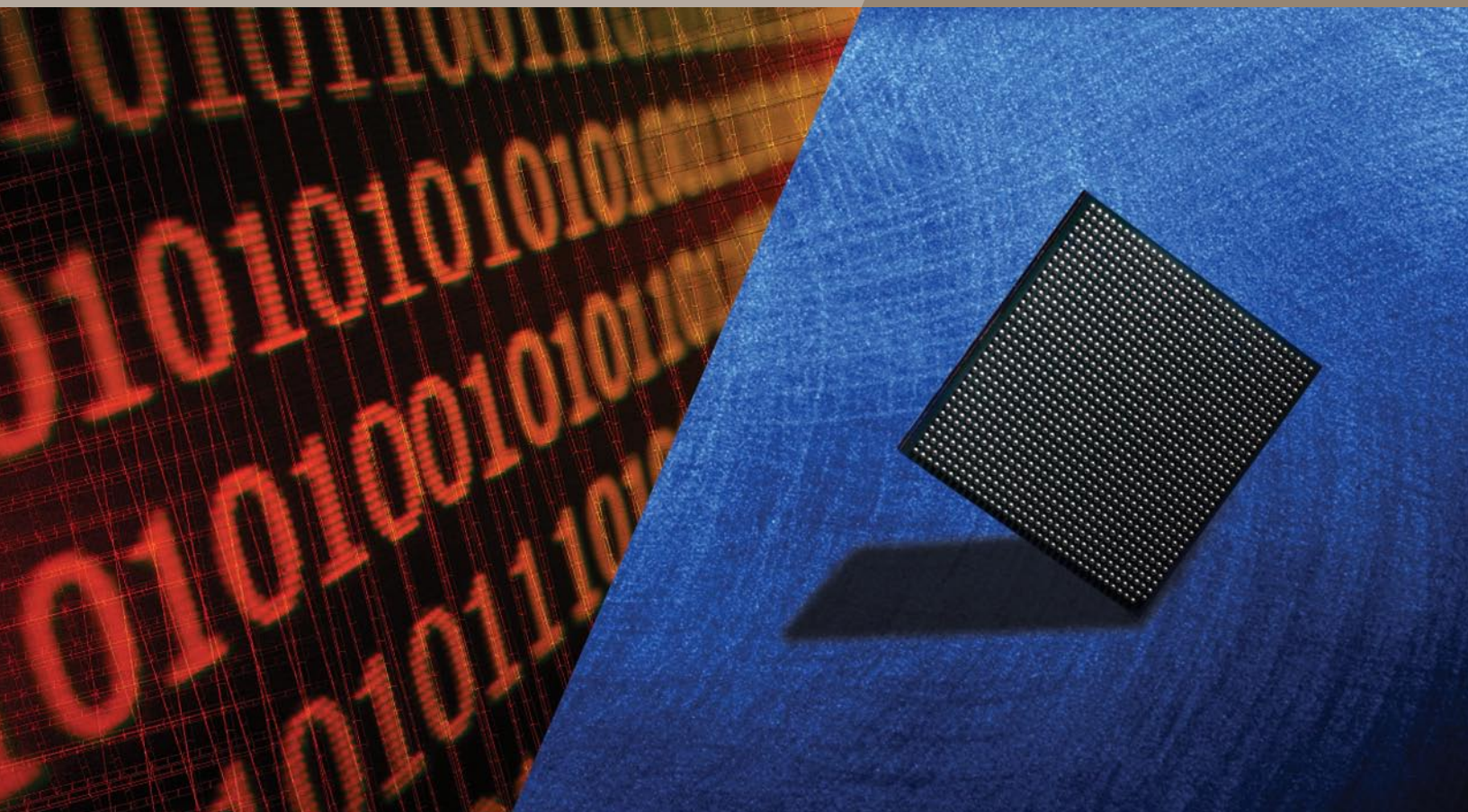


Janus MILS, Multi-Channel, Programmable Cryptographic Engine



Janus is soon to be a NSA certified Type 1, MILS cryptographic engine.

Janus is an embeddable, MILS multi-channel, programmable cryptographic engine for DoD equipment requiring high-assurance cryptographic processing. Developed to enable compliance with the Crypto Modernization Initiatives requiring Assured Security Robustness, Crypto-Algorithm Support, Interoperability, Releasability, Programmability, End Cryptographic Unit (ECU) Management, and KMI Compatibility needs.

KEY BENEFITS:

- › The Janus MCM architecture offers a smaller, lighter solution that uses less power supporting complete user programmability
- › High-speed encryption and decryption of digital voice and data, multi-channel, half-duplex operation and MILS operation for simultaneous processing of unclassified up to top secret code word data
- › Concurrent operation of both modern and legacy algorithms to ensure a seamless crypto modernization transition of net centric operational requirements

KEY FEATURES:

- › Fully programmable algorithm and application software
- › High-speed encryption and decryption
- › MILS capable unclassified up through top secret code word (simultaneous)
- › Multi-channel capabilities (5)
- › State-of-the-art MCM (on board RAM, flash, randomizer, and I/O)
- › CIK, CRK, DS-101 and DS-102 interface
- › Benign key fill

**Rockwell
Collins**

Building trust every day

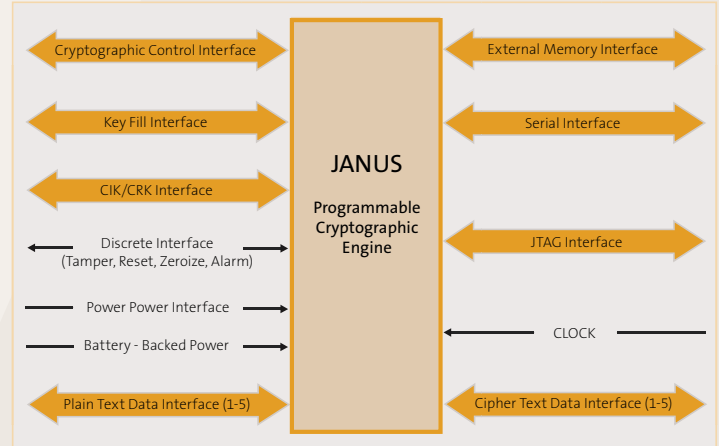
- › Active power management
- › Small form factor (45mm x 45mm package)
- › Anti-tamper
- › TTNT compliant

KEY MANAGEMENT

Janus provides DS-101, DS-102 and benign fill key management capability to meet both legacy and future cryptographic modernization requirements. Janus enables keys to be loaded in either red or black formats, stored black, and selectively zeroized, as well as supports session key generation using Firefly and Enhanced Firefly. Rockwell Collins' internal Advanced Architecture MicroProcessor 7 Government Version (AAMP7G) is integral to Janus' key management ability.

The AAMP7G was certified in May 2005 by the National Security Agency (NSA) as a Multiple Independent Levels of Security (MILS) device for use in cryptographic applications. Janus MILS capability is designed in and assured through the AAMP7G's unique microarchitecture which employs a secure, hardware-based separation kernel. The Janus MCM has a robust on-board random number generator required for algorithm processing and key management functions.

BLOCK DIAGRAM



Building trust every day.

Rockwell Collins delivers smart communication and aviation electronics solutions to customers worldwide. Backed by a global network of service and support, we stand committed to putting technology and practical innovation to work for you whenever and wherever you need us. In this way, working together, we build trust. Every day.

For more information contact:

Rockwell Collins
 400 Collins Road NE
 Cedar Rapids, Iowa 52498
 800.321.2223
 319.295.5100
 Fax: 319.295.4777
 E-mail: collins@rockwellcollins.com
 Web site: www.rockwellcollins.com/gs

Algorithms	Equipments
Accordion 1.3	CTIC
Accordion 3.0	KG-3X
AES-128/192/256	KG-40
BATON	KG-84A/C
CRAYON	KGV-11
CRC64-ISO	KGV-68
DES/3-DES	KIV-7
ENHANCED FIREFLY	KY-100
FIREFLY	KY-57
JOSEKI	KY-58
KEESE	KY-99
MEDLEY	KYV-5
SAVILLE	NOBLEMAN
SHA-1	RAILMAN
SHILLELAGH	
WEASEL	



Building trust every day