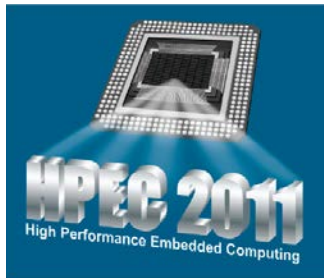




# A Reconfigurable Advanced Tamper Resistant Embedded Processing Platform

Jason Fritz, Michael Bonato, David French and Larry Scally  
jason.fritz@coloradoengineeringinc.com

September 22, 2011



<http://www.coloradoengineeringinc.com>

## SBIR DATA RIGHTS

**Contractor Name:** Colorado Engineering Inc. (CEI)  
**Contractor Address:** 1310 United Heights, Suite 105, Colorado Springs, CO 80921  
**Expiration of SBIR Data Rights:** Expires 5 years after completion of project work for this or any follow-on SBIR contract, whichever is later.

This presentation contains data developed by Colorado Engineering under SBIR contract HQ0006-08-C-7908. The Government's rights to use, modify, reproduce, release, perform, display, or disclose technical data or computer software marked with this legend are restricted during the period shown as provided in paragraph (b)(4) of the Rights in Noncommercial Technical Data and Computer Software - Small Business Innovation Research (SBIR) Program clause contained in the above identified contract. No restrictions apply after the expiration date shown above. Any reproduction of technical data, computer software, or portions thereof marked with this legend must also reproduce the markings.

Export or re-export of CEI products may be subject to restrictions and requirements of US export laws and regulations and may require advance authorization from the US Government.

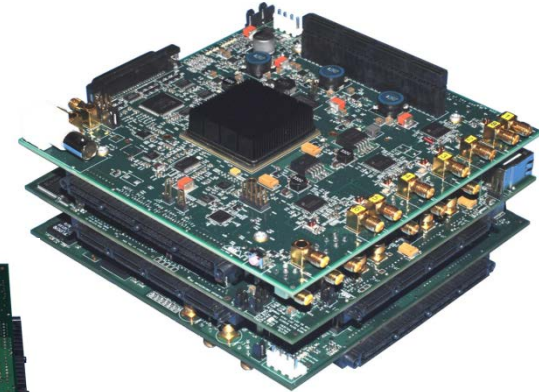
# Reconfigurable Advanced Rapid-prototype Environment (RARE)



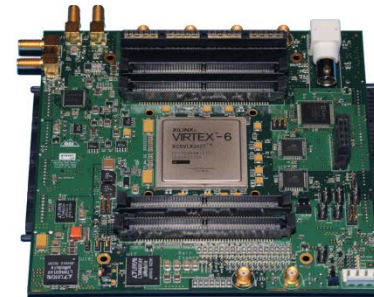
- Modular embedded computing
- Flexibility to fit both spatial and processing requirements
- Connectivity via standard interfaces (e.g., PCIe, LVDS)
- Programming via a model-based SDK
- Modules for general purpose processing, ADC, DAC, platform interface (e.g., aircraft, ship), 10 GbE, system clock control



2 Processor modules connected side-by-side, each with a PowerPC and Virtex-6.



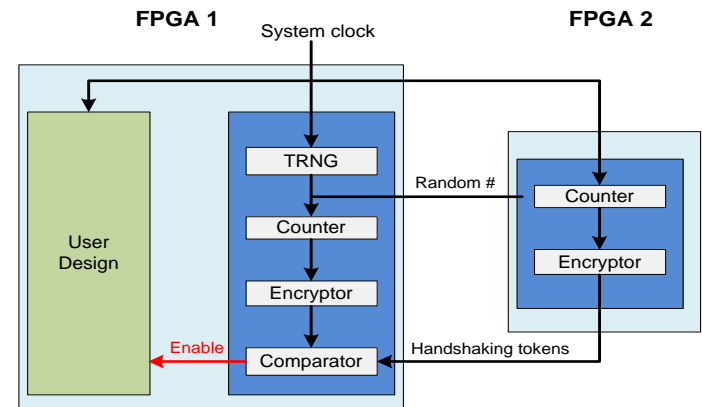
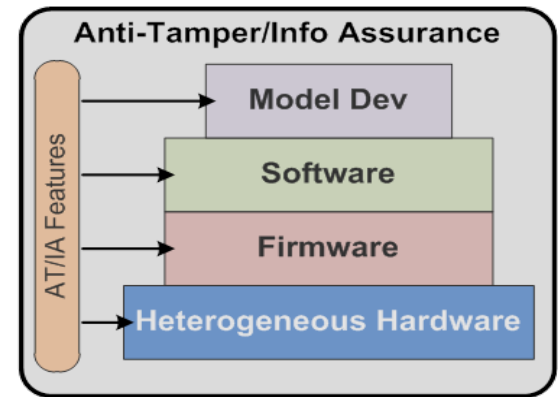
A vertical stack of ADC (top), Processor and DAC modules. The ADC provides 10 channels at 16-bits, 160 MSa/s



A 250 MHz, 16-bit DAC module with two independent channels

# Protection

- Anti-Tamper/Information Assurance features are added at all levels of a hardware based system
- Heterogeneous hardware platform provides the infrastructure to the software and firmware
- Development using model-based software development kit
- AT/IA features are integrated at all levels
- Utilize security features in Virtex-6 (defense grade), PPC460SX, flash memories



An example mutual authentication scheme between module FPGAs (across boards) to assure that the system contains the appropriate, as-designed components. Correct handshaking tokens must be received for normal operations.



# MCU System Health and Status Monitoring

- Each RARE module contains MCUs connected to global I2C bus
- Master-slave configuration when multiple modules present
- I2C protocol provides details on network discovery and management plus a mechanism to broadcast status to all modules
- MCUs sequentially power up each module and control FPGA booting if applicable
- MCUs can shut down individual modules to protect system from overheating, save power, etc.
- Data are stored in EEPROMs to enable extraction after a full power shutdown
- Monitors all voltage rails, current from the switched power supply and up to five temperature sensors
- Fully programmable
- Can utilize MCU security features