A Reconfigurable Advanced Tamper Resistant Embedded Processing Platform

Jason Fritz, Michael Bonato, David French, Larry Scally
Colorado Engineering, Inc.
{jason.fritz, michael.bonato, david.french,larry.scally}@coloradoengineeringinc.com

Introduction

There are many instances where complex sensor suites are required under severe size, weight and power (SWaP) constraints including unmanned systems, helicopters and missiles. These systems, however, can fall into the possession of unauthorized personnel either through accident or hostile means. In order for the U.S. to maintain technological superiority, it is paramount that the technical content be protected [1] as required by the Department of Defense Directive 5200.39. This directive defines Critical Program Information (CPI) as "Elements or components of an RDA *[research, development and acquisition]* program that, if compromised, could cause significant degradation in mission effectiveness; shorten the expected combat-effective life of the system; reduce technological advantage; significantly alter program direction; or enable an adversary to defeat, counter, copy, or reverse engineer the technology or capability." Protection is achieved by incorporating anti-tamper *[AT]* technology which can be hardware based, software based or a combination of the two.

Reconfigurable Processing Architecture

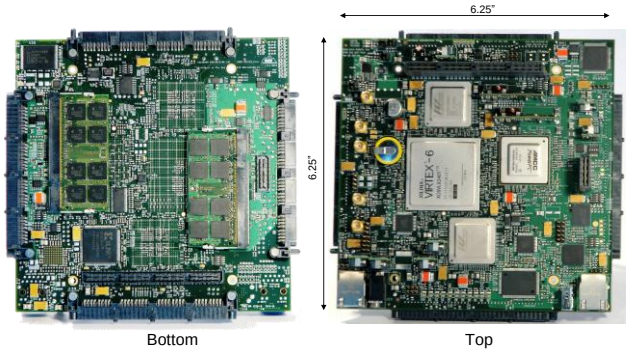

Figure 1: Existing Reconfigurable Advanced Rapid-prototyping Environment (RARE) processor board with a PowerPC CPU and Virtex 6 FPGA

In order to meet these SWaP and protection requirements, Colorado Engineering, Inc. is enhancing their existing Reconfigurable Advanced Rapid-prototyping Environment (RARE) family of processing modules [2] with more advanced processing units and anti-tamper technologies. The award-winning RARE technology was originally developed under contract with the Missile Defense Agency as a scalable, compact digital radar receiver/exciter to meet tight SWaP requirements. The family of RARE modules includes a processor (see Figure 1), 10 channel analog to digital (A/D) converter, 2 channel digital to analog (D/A) converter and various interfaces (e.g., 10 GB ethernet). A Xilinx Virtex®-6 FPGA is included on the Processor, A/D and D/A modules including up to 4 GB of DDR2 memory for the Processor and A/D modules. The processor CPU is a PowerPC (PPC-460SX) running at speeds up to 1.2 GHz. Each module contains a combination of connectors in all 3 dimensions allowing them to be connected in a variety of configurations; they do not require a backplane as shown in Figure 2. Communication and data flow is achieved over a variety of standard formats such as LVDS, PCI express (PCIe), SerDes and I^2C. Table 1 provides the input/output bandwidth of the primary data connections in each of the 3 dimensions and the total bandwidth. All RARE modules are 15.9 cm^2 and weigh less than 360 g.

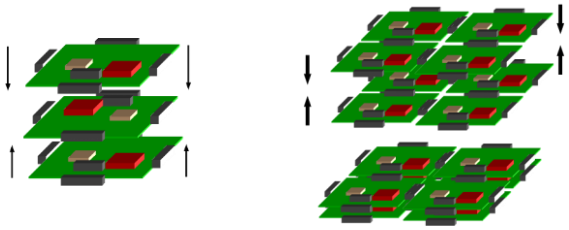

Figure 2: RARE Module interconnect options for system footprint flexibility

Table 1. RARE I/O Bandwidth by Connector in MB/s

RARE Con-nector	Half Duplex	Full Duplex			Total Bandwidth
	LVDS Total	PCIe FPGA	PCIe PPC	SerDes FPGA	
X	2,625	2,000	2,000	0	6,625
Y	2,625	0	2,000	0	4,625
Z	3,250	2,000	2,000	1,000	8,250

There are two micro controllers (MC) on each board that communicate with other connected modules over an I^2C bus monitoring system status, temperature and voltage rails. When a set of RARE modules are connected, which can include multiple copies of each type to accommodate bandwidth needs, one MC is designated as the master, typically communicating directly to a CPU, while the remaining MCs are slaves. Board ambient temperature as well as FPGA and CPU temperatures are monitored. System status, including faults, tamper detection, unsafe conditions (e.g., radar duty cycle too high) and other programmable features are continually monitored with the ability to shut down power to a given module.

Under several DoD SBIR programs, Colorado Engineering is currently designing the next generation of RARE processing technology. The single core PPC CPU is slated

to be upgraded to a Freescale QorIQ™ CPU with built-in standard interfaces. Future options include advanced processors such as DSPs, GPUs or combinations of several types.

Anti-Tamper Technologies

There are numerous technologies for implementing anti-tamper schemes that all have pros and cons [3] and one must perform a threat analysis to determine the requirements. While there is no "best" individual method, a hybrid hardware and software solution typically offers the best overall solution. One that is currently available for RARE is the addition of security features for the PPC-460SX. Hardware acceleration for IEEE 1619 encryption/decryption is available for data stored on a connected medium. The built-in Turbo Security engine option provides protection for throughput data using DES, 3DES, AES, and ARC-4 encryption plus MD-5, SHA-1 and SHA-2 (SHA-256, SHA-384, SHA-512) hashing.

The near future will see a release of the XilinxVirtex®-6 defense grade components containing silicon AT features that are pin compatible with the current models. These Xilinx features, in addition to the MC monitoring of board health discussed above, provide a wide array of AT options without requiring new module layouts. The Xilinx silicon AT features include the following: AES 256-bit encryption (volatile key – Battery Backed RAM and non-volatile key - eFuse), hardened readback disabling circuitry, single event upset (SEU) Checker, JTAG disable/monitor, internal keyclear, internal config memory clearing, unique identifier (Device DNA), HMAC bitstream authentication, on-chip temperature and voltage monitoring, PROG intercept and unique identifier (User eFuse). With the ability to shut down some or all modules in the system when suspicious temperature, voltage, clock changes or even detection of component removal are detected, the microcontrollers offer another layer of protection that works cooperatively with the FPGA.

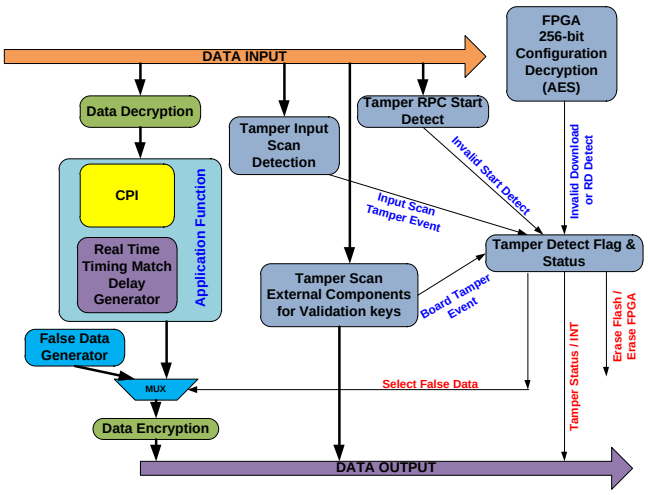

Figure 3. Block diagram of the FPGA architecture for CPI protection. The CPI can be from the same CCA or from a legacy system

One top-level scheme for protection of CPI from an unprotected system through a RARE processor is depicted in Figure 3. Software CPI is identified, extracted from the binary executable and disassembled (based on original system architecture). The CPI assembly code can then be analyzed for dependencies and data flow whose logic can be implemented as a shared library module within the secured FPGA. A Remote Procedure Call (RPC) from the original binary is then used to pass execution to the FPGA. If tampering is detected by any means, including unauthorized attempts to execute the CPI core, the tamper detection flag is set and either the output data is intentionally corrupted or all memory, data and FPGA configuration is destroyed.

With the processor enhancements currently in development, a system comprised entirely of RARE modules will incorporate further AT technology. In particular, the Freescale QorIQ™ CPUs include a Trust Architecture to support and maintain a trusted environment from boot [4]. The Trust Architecture offers the following features: unauthorized modifications to software and system configuration can be detected; confidential code, factory installed keys and other system secrets are protected; multicore CPUs enforce barriers between partitions; and once trusted software is authenticated on a partition, modifications can be quickly detected or prevented. On a board level, the addition of "tamper-reactive" secure key storage using a battery backed integrated circuit such as the PDS8006 from Priva Technologies can further enhance the security of the system. As a whole, these technologies will provide several layers of protection in combination with pure software AT tactics including encryption wrappers, code obfuscation, software watermarking and guarding [3].

Conclusions

RARE combines heterogeneous high performance computing, ease of programmability, and commercial standard I/O flexibility to facilitate cost-effective, scalable processing for SWaP-constrained applications. With the advent of state-of-the-art AT and security technology in CPUs and FPGAs, a RARE system can provide a high level of protection for CPI, adding tools for software and firmware developers. In addition, a RARE processor can be added to unprotected legacy systems to incorporate AT in those.

References

[1] A. F. Huber II and J. M. Scott, "The role and nature of anti-tamper techniques in u.s. defense acquisition," *Acq. Rev. Quar.*, pp. 355–368, 1999.

[2] M. J. Bonato, D. French, J. Fritz, and L. Scally, "Modular, scalable computing for systems with tight SWaP constraints," in *High Performance Embedded Computing Workshop HPEC*, 2011, submitted.

[3] M. Atallah, E. Bryant, and M. Stytz, "A survey of anti-tamper technologies," *Crosstalk J. Def. Soft. Eng.*, vol. 17, no. 11, pp. 12–16, Nov 2004.

[4] "An introduction to the QorIQ platform's trust architecture," Freescale Semiconductor, White Paper QORIQTAWP, May 2011.