Security Separation of Cores in Multi-core Architecture

The semiconductor industry has arguably reached the point where security is not just an application level requirement, but a processor level requirement as well. A small but specialized industry has addressed several government needs for high speed classified processing, but more is needed. Specialized ASIC design with electromagnetic and air ‘gaps’ is becoming an expensive and highly constrained approach, and more tools are needed. The first tools to enable this data separation have been in software and operating systems, but rounding out that portfolio is a reconfigurable multi-core firewall capability in the Acalis secure processor.

Multi-core Trends

There are two very distinct drivers for multi-core, or multi-processor operation. The one most people are familiar with is the trend towards parallelizing operation to increase performance for high end computing. This is a performance trend, often cited as an alternative to persistent investment in increasing clock speed and reducing junction size in semiconductors.

The second trend is to partition operations within embedded computers for the purpose of increasing security and increasing control over access to sensitive information. This trend, in turn, can be divided into two different approaches towards partitioning: physical partitioning of operating cores, and partitioning applications into different virtual machines within a single core.

The development cost and implementation advantages of virtualization make it an attractive approach towards application and communication layer security. It also promises to benefit from rapid evolution as it is deployed in consumer and financial applications, and supported by larger eco-systems of operating systems and applications. There are several developers currently supporting virtual machine many-core operation and ‘hypervisors’ to manage them.

However, the benefits and higher security opportunities of physical on-chip core separation and security management has yet to be explored for extremely high security applications. There are very few commercial offerings today with multi-core configurable physical firewalling capabilities.

Of even higher potential value is a combination of physically separated cores operating virtual machines, overlaying hardware and software security features. This brings the security features of both approaches into a single, high security system.

Multiple Independent Levels of Security

There is a variety of reasons to separate out application tasks into separate operating cores or virtual machines. In a typical commercial application, you may want one core or virtual machine performing a customer transaction, but a separate core or virtual machine accessing sensitive customer data or financial information before passing it along in an encrypted message.

This separation capability has applications in industrial safety and security, where some operations require fast or understood processing speed or latency, while others require high degrees of redundancy and parameter checking before operating physical machinery or chemical processes.

October 2009, ver. 0.0
At the highest levels of sensitive information or operating safety are military transmissions, intelligence agency information, and government trusted networks. These typically require independently verified physical separation and controls between different levels of classified information, which is a difficult enough task when discussing single core processors.

Standards for assessing the security of these applications include a ‘Separation Kernel Protection Profile’ (SKPP) for virtual separation, and a variety of standards governing ‘Multiple Independent Levels of Security’ (MILS) for government applications.

**MILS in a System-on-a-Chip**

Translating MILS type requirements into a single device is a difficult issue for government security assessors. Several government labs and defense contractors have experience with ASSP products and dedicated encrypters, but limited experience with separation in programmable logic, soft processors, and embedded processors with reconfigurable parameters.

Dedicated ASIC logic will always exist for the highest levels of security and separation requirements, but programmable firewalls and memory segmented virtual machines offer a new toolset for security engineers to trade flexibility and security.

**Reconfigurable Multi-Core Firewalls**

The options for executing multi-core separation and firewalls in the Acalis secure processor allow for a wide variety of security applications. Here we will describe the options available for the dual core CPU872 device, and some notes on how this will scale to devices with more than two cores.

**How Acalis Separation Works**

![Figure 1. Example of Firewall Settings on a Single PowerPC Core](image)

The separation capabilities of the Acalis secure processor are architected into the device. The entire architecture, including every process attached to each PowerPC operating core, is memory mapped. The majority of this memory map, in turn, is assigned an access setting in configuration.

Looking only at each PowerPC core in the Acalis secure processer, a security engineer defines the software accesses to each service individually, including whether access is read, write, or both. In the example above, the PowerPC core can access all of its own services, but outside
cores can only write to this core’s memory space. The message passing interface is enabled to send and receive messages from this core as well.

![Diagram showing firewall settings on two PowerPC cores.](image)

**Figure 2. Application Example with Firewall Settings on Two PowerPC Cores**

The second diagram above shows an example of how two cores might be configured for a security application. Core A (on the left) is a data processor utilizes all of its own resources, and utilizes the MPI interface for interaction with other processors and data connections. Here a first decryption or unscrambling might take place. The data is then sent via encrypted MPI to the eDRAM on core B on the right. Core B is almost entirely isolated in this instance and access is limited to a small address space. This core can implement encryption or other sensitive operation on the data.

Isolating Cores vs. Separating Cores

The application example above shows how the configurability of the firewall settings in the Acalis Sentry® allows the user to set security accesses in the PowerPC operating cores for a variety of purposes. A core can be entirely isolated from all other operations on the device except for a small address space, for example. More importantly, the user has a variety of options for defining all communications between two operating cores in a red-black or security isolation environment. This communication can be anything from MPI to Ethernet to streaming data. Individual firewall settings can be preconfigured so that they are not changeable in software – only through device configuration by the Acalis Sentry.

Comparison to the Virtualization Approach

There is an important comparison to be made between physical core firewalls and virtual machine separation. But as noted earlier, this comparison is not made as a trade study between which approach is more secure or cost effective. Rather, this comparison is shown in order to highlight the different ways in which each approach is secure, and the benefits of employing both hardware separation and application virtualization within a system as a layered security approach.

Whenever a new virtual instance is created on a processor core, it is created to generate a security separation from other operating threads. Creating new virtual machine threads on a single processor core increases the taskload on that processor core. Loading a secure application on a different core, and configuring that core with the right security settings, will not impact the performance on the original core. If the system has both configurable operating cores
and a secure operating system, both options are available to the system.

Employing both virtual machine operation (with security segmented memory) and hardware core separation in combination requires a highly technical systematic design approach. This approach will take advantage of thread isolation capabilities of secure operating systems like VX Works and Integrity, and the performance advantages of hardware core firewalls.

**Advantage: Reconfiguring Security Without Impacting Performance**

As this exercise has shown, there is a distinct advantage in reconfigurable hardware cores in that application performance does not change as security configuration changes. Entire processor threads can still be dedicated to the secure operation, without sharing processor interrupts with a new virtual machine. Operations that are sensitive to performance benchmarks can perform security reconfigurations without creating other timing or performance based security vulnerabilities.

**Scaling to Large Multi-core**

An important principle of both physical separation schemes and virtualization is the ability to scale the model to many cores and many virtual machines. This is primarily a tools issue. Where a great deal of investment is already being made in solving the general problem and approach to multi-core development, CPU Tech has focused on the problem of defining the problem space of multi-core secure interoperability, defining the security parameters required for tool design, and making this tool set available to users in the Acalis Sentry® Tool Kit.

This tool set has been developed to enable firewall and access settings for the Acalis CPU872 dual-core secure processor. However, its design is aimed at enabling both bus and connection level security settings for massively multi-core projects, as well as simple profile templates enabling several common security applications like encrypted communications, handling of sensitive input data like customer information, and data fusion from various sensitive data sources. The diagram below shows some of the many ways information and processes can be segregated using the Acalis SDK and Sentry Tool Kit.
Figure 3. Different types of Core Security Separation Possible with Acalis Multi-Core Devices

Security Certifications and Assessments

Unfortunately for developers of security technologies, user adoption is primarily driven by third party assessments and certifications. These assessments and certifications typically lag the technology cycle. New security technologies and approaches, no matter how novel, tend to experience abnormally long adoption cycles.

This is the case for physical core separation. In theory, there are several key features of the Acalis core separation security that will simplify certifications for encryption modules or common criteria system assessments. However, this assertion will need to be scrutinized by both certification lab professionals, as well as drafters of security standards.
References:
