Secure ASIC Architecture for Optimized Utilization of a Trusted Supply Chain for Common Architecture A&D Applications

Ezra Hall, Ray Eberhard, Jeff Magee, Gary Reuland, Sebastian Ventrone
GLOBALFOUNDRIES
Essex Junction, Vermont, 05452

Abstract: *Department of Defense Policy 5200.44 requires Trusted sourcing for mission critical integrated circuits, yet economic forces have caused the semiconductor industry to predominantly shift overseas. Concurrently, time to market and complex system requirements are increasingly outside the budget range of standalone DoD projects. This paper presents options for addressing these challenges and proposes a flexible Secure ASIC architecture.*

Keywords: Trusted; Secure; SoC; ASIC

Summary: A proposed shared architecture library and integration methodology will be presented, along with the ability to add trusted Functions, within a scalable controlled environment. This solution includes a platform for common methodology, IP, and integration techniques, to reduce cost/risk across programs, and that would be managed by a center of competency (COC) within the US Government (USG), in close partnership with industry.

Overview

USG programs have historically satisfied unique program needs with single end use custom ASICs; however, long design cycle times and high cost, combined with limited reuse capabilities, have slowed the overall growth of ASIC usage within the A&D (Aerospace & Defense) sector. This has resulted in continued reliance upon FPGAs for the majority of USG programs, negatively impacting the size weight and power (SWAP) of such solutions.

Concern grows that adversaries leveraging commercial off the shelf IP could achieve advantage by riding the wave of leading edge commercial semiconductor offerings available overseas. More recent A&D ASIC designs have targeted multiple end-use DoD programs, with enough success that this multi end use model has viability. Further leverage of this approach can help drive the trajectory for continued asymmetrical advantage to USG programs, by more aggressively targeting leading edge technologies.

This paper proposes the definition of secure SoC architectures and subsystems that maximally leverage leading edge technologies, complex IP (including device and application security IP), integration, and implementation capabilities to deliver a superior secure SoC solution to A&D applications to better balance configurability, cost, and availability. These common architectures would be targeted to be both scalable and flexible through programmability and/or customizability, including application specific IP, for use in multiple A&D end use applications. Furthermore, a product roadmap must be comprehended as part of this platform, offering A&D programs a solution to their significant Diminishing Materials Supply (DMS) problem, and more direct migration paths to further reduce SWAP with increased functionality through adoption of advanced technologies for component upgrades.

Current Solutions

The majority of A&D custom ASIC solutions align to end-use specific ASICs that leverage a selected technology for a single program. Due to architecture and technology complexity, significant chip integration and verification efforts are required. Coupled with USG fiscal year phased funding models, the result is lengthy multi year development cycles. Such architectures typically feature an embedded processor core, often a general purpose DSP, several high speed serial links, non-volatile memory (NVM), and large amounts of memory. These designs are expensive and complex, requiring years of testing, re-releasing and qualification on targeted platforms, and are typically node locked to the original semiconductor technology selected without migration paths forward to newer technologies.

Recognizing such expense and delay to market concerns, a major FPGA vendor has offered an FPGA specifically targeting the A&D market. Architecturally, this offering includes an ARM dual core Cortex 9, a Neon Floating Point coprocessor, DDR family High speed serial links, USB and I2C IOs, and programmable Interrupts. Additionally, AES and SHA 256 bit decryption, and an authentication macro for secure boot, is also available. There are four versions of the design with varying amounts of FPGA fabric ranging from 85K to 444K programmable logic cells, depending upon the targeted price point. FPGA solutions allow for low entry cost but result in significantly higher SWAP characteristics in comparison to an ASIC solution and offer no flexibility for adding new IP blocks not originally included in the architecture.

A secure SoC needs to provide both technical and economic benefit over these two existing solutions for adoption to occur. Additionally, a well-developed roadmap to future secure SoCs, leveraging the value add of future advanced technology nodes and IP, must be comprehended. Examples of current GLOBALFOUNDRIES[1] (GF) value-add in technology and IP that can be leveraged for a secure SoC, is captured in the family of leading edge HSS cores, industry leading 2.5D and 3D integration offerings, dense and high

speed embedded memory options including TCAMs, and other leading edge IP and features at 14nm. This rich offering is ideally matched to the technology needs of a secure SoC.

Security Features

A secure SoC requires that a platform, encompassing both the silicon and enabling software solution, be developed in concert. The goal of the incorporated security layers is to guard and prevent against a broad range of attacks extending from physical to programming intrusions. To provide this layer of protection, a broad suite of IP and onboard software needs to be created. Examples include:

- Hardware based encryption engine
- Hardware based random number generation
- Encryption key storage (persistent storage within the Secure SoC)
- Address authentication
- PUF (physically un-cloneable function)
- Security sensor suite and state controller
- Secure boot code and secure ROM
- Trusted board support package
- Silicon DNA or Fingerprinting

The combination of these elements forms a cohesive set of security layers, protecting both the physical device and code running on the device from attack.

Architecture Features

A Secure SoC will require additional architectural features to support as broad a range of A&D end use applications as possible. This set of functions will need to be configurable, and have the ability to isolate and power-gate the portions of the design that are not required for a given end use for reduced power consumption. The product will need the ability to be provisioned for end use through programming at wafer or module final test, at system build, and/or in the field during system use. This flexibility would drive an innovative eFPGA or other programmable fabric, along with sufficient embedded NVM for crypto keys or other provisioning needs including CPI. To provide this level of SoC functionality, the following features/IP requirements are anticipated:

- General Purpose processor such as ARM
- On-chip DSP
- High speed serial link (HSS) capable of supporting a broad range of standards
- eFPGA core(s) or other programmable fabric, allocated toward both security and user defined functions
- On-chip power management system
- High speed analog convertors
- Programmable clocking
- On-chip communication busses
- JTAG architecture ports

The list of features and function will depend upon programs selected for the partnership. A joint USG - industry partnership could enable an optimization of architectural features across selected programs, to arrive at an optimized balance between configurability, up-front cost, and production costs.

Intrusion / Tamper Detection

GF technology can also be leveraged to provide a suite of sensors and devices specially tuned for intrusion detection, forming a Secure Foundation IP portfolio (SFIP) for inclusion in the architecture. Examples of sensor IP include:

- Power supply monitor (noise, voltage, . . .)
- Clock quality monitor (jitter, frequency, . . .)
- Temperature & voltage sensors
- Light and EMF sensors
- Substrate intrusion monitor
- Alpha/gamma radiation detector

Exemplary Implementation

Figure 1, below, captures one of many possible secure SoC architectural configurations.

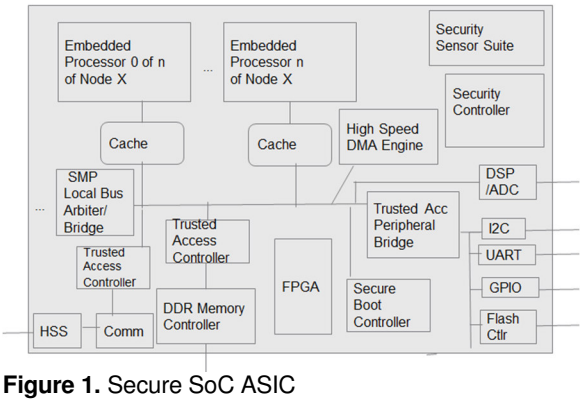

Figure 1. Secure SoC ASIC

To enable end use provisioning, a software suite is necessary to define each configuration and enable programing. Each end use program would define a configuration, and provisioning could occur at the factory during final manufacturing test, and/or in system build and/or in field use. In this manner, each program can determine the optimal point in the end-to-end flow for provisioning and addition of CPI.

Embedded Secure FPGA

Embedded FPGA (eFPGA), or other programmable fabric capability, is an enabler to product customization for end uses. The eFPGA architecture will depend upon requirements of selected partner programs, and the desired flexibility of the SoC implementation. Determining how best to partition and distribute the eFPGA within the subsystems, including connection to the SoC buss, and security fabric/circuits, will require optimization and system modeling.

eFPGA cores from existing vendors are ideal candidates to enable such programmable fabric. Menta[2] for example has established eFPGA architectures utilizing the leading edge 14LPP technology available from GF. This offering includes a development tool set and an architecture that allows for eFPGA partitioning across the secure SoC, thus enabling optimization to create the proper bus interfaces and other requirements. See Figure 2 for one such implementation.

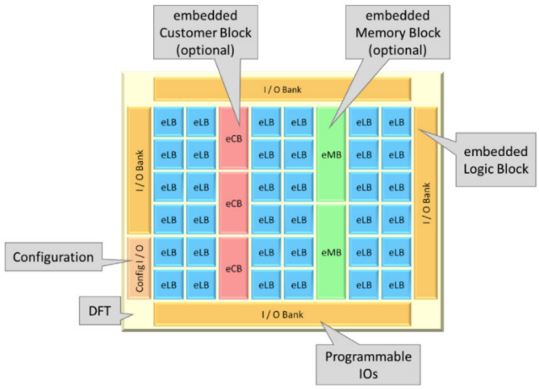

Figure 2. Example eFPGA partitioning

As an alternative to eFPGA, a configurable metal wiring fabric could be utilized, whereby each customized design modifies only several wiring levels to complete the chip provisioning. In this manner only several of the 60-70 mask levels would need to be changed for each end use configuration at significant cost and schedule savings in comparison to full dedicated ASIC designs for each end use.

Memory and Bus Protocols

The communication and bus protocols can be configured to provide maximum flexibility and the ability to reroute data from high congestion areas to lower congestion areas. New and novel bus protocols could be architected to provide a flexible inter-core and memory transfer mechanism, with the ability to dynamically allocate bus bandwidth between the different units and memory and cache subsystems. A bus model of the system could be created to model the bandwidth requirements of the processor(s), eFPGA fabric, and memory/caches, to determine the number of lanes and levels of data transfer.

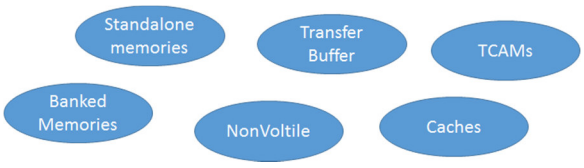

Figure 3. Memory Units

The amount and type of memory required will be a function of the end uses. Figure 3 identifies typical memory types required for A&D applications, with amount varying according to each end use. Some applications require CAMs, whereas others (such as 5G) require new dense serial transfer memory buffers and non-volatile memory. The memory types and configurations available would be optimized for the requirements of partner programs selected.

Additional Flexibility with System on Module

A significant shortfall for use of standard products, which applies to both commercial and A&D end uses, is restricting the system designer to the IP building blocks implemented in the standard products. A single SoC solution cannot be defined that satisfies all possible end uses as the die size/power/cost will exceed practical limits. Conversely, a SoC lacking certain key enabling IP may preclude re-use in a future program. A potential solution to achieve a balance of standardized SoC content while allowing integration of custom IP is to leverage 2.5D and 3D assemblies to incorporate additional die level components into the end product module. An additional benefit of this solution is enabling the combination of disparate semiconductor technologies, such as 14LPP with RFCMOS or RFSOI, and even Silicon Photonics. In essence, creating a configurable system on carrier solution for maximum flexibility.

An alternate and more flexible approach involves derivative secure SoC architectures, to include such additional/alternate IP in design re-spins of the original SoC architecture. Such an approach would allow for re-use of the original secure SoC architecture, at a lower cost than a full new design.

USG - Industry Collaboration

To implement this proposal will require close collaboration between the USG and commercial suppliers. To effectively manage this, and other USG related semiconductor procurement efforts, it is recommended the USG adopt best practices exercised by successful US based fabless semiconductor companies, and establish a center of competency (COC) for semiconductors. The COC would provide significant advantage to the USG in achieving cross program collaboration including; definition of standards, common architecture committee, program management expertise for efficient procurement from industry, and reduction of redundant functions within the DoD ecosystem. The authors of this paper observe that DMEA, in its role administering the Trusted Access Program Office[3], would be well positioned to take on this effort.

Selected industry partners must have expertise in development and delivery of first time right silicon, in engagement models that enables performers on USG programs to focus on their core competencies for system architectures, while offloading the technology implementation details to the supplier(s). Required services would include:

- Turnkey IP, SoC Subsystem, and/or Full SoC development capabilities
- Test Structure insertion

- Place & Route, timing closure
- Signal Integrity analysis
- Power optimization and integrity analysis
- LVS/DRC checking
- Logic Verification
- Packaging, test, and reliability screening

GLOBALFOUNDRIES' FX-14[4] ASIC platform at the 14nm node satisfies these requirements with a Production-proven design methodology that builds on a strong record of first-time-right results to help reduce development costs and time-to-market

Such services could individually be engaged, each spanning commercial to Trusted handling levels, as appropriate for balancing availability and cost vs. Integrity and Confidentiality. Additionally, a "Hybrid Trust" model approach could be adopted, whereby IP elements and design blocks sourced from the commercial ecosystem are synthesized and implemented on a commercial platform, and then integrated within a Trusted Design Center with Trusted elements of the design. In this manner, any classified or sensitive portions of the design are protected from a Confidentiality and Integrity perspective within the Trusted domain, and other portions of the design of commercial origin are protected at an appropriate level and not more than necessary. This approach could reduce cost while simultaneously increasing Availability and improving schedule.

Conclusion

Collaboration for common architectural elements and IP investments are critical to leveraging advanced technology, while simultaneously minimizing budget requirements, and gaining access to constrained availability from suppliers. To manage the complexities of this business, a USG Center of Competency for semiconductors is necessary, to apply deep semiconductor related expertise to cross program collaboration, with robust program management of suppliers, in a manner similar to how successful commercial fabless semiconductor companies perform. With this approach, best commercial industry practices can be adopted by the USG, to navigate evolving threat vectors, Availability, and other emerging factors, to bolster U.S. asymmetrical advantage.

References

1. http://www.globalfoundries.com/
2. http://www.menta-efpga.com/
3. http://www.dmea.osd.mil/tapo.html
4. http://www.globalfoundries.com/technology-solutions/asics